(特許協力条約に基づいて公開された国際出願)

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003年7月17日 (17.07.2003)

PCT

(10) 国際公開番号
WO 03/058411 A1

(51) 国際特許分類[7]: G06F 1/00, 9/06

(21) 国際出願番号: PCT/JP03/00035

(22) 国際出願日: 2003年1月7日 (07.01.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-1843 2002年1月8日 (08.01.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社エヌ・ティ・ティ・ドコモ (NTT DOCOMO, INC.) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目11番1号 Tokyo (JP).

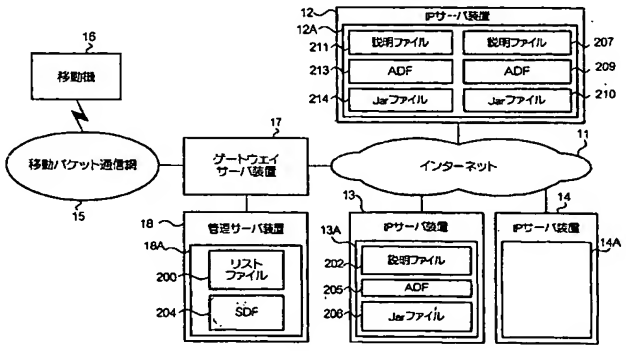
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 山田 和宏 (YAMADA,Kazuhiro) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 渡邊 信之 (WATANABE,Nobuyuki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 津田 雅之 (TSUDA,Masayuki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 神谷 太 (KAMIYA,Dai) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 浅井 真生 (ASAI,Mao) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 三浦 史光 (MIURA,Fumiaki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 鷲尾 諭 (WASHIO,Satoshi) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二丁目１１番１号 山王パークタワー 株式会社エヌ・ティ・ティ・ドコモ 知的財産部内 Tokyo (JP). 富岡 淳樹 (TOMIOKA,Atsuki) [JP/JP]; 〒100-6150 東京都 千代田区 永田町二

[続葉有]

(54) Title: CONTENT DELIVERY METHOD AND CONTENT DELIVERY SYSTEM

(54) 発明の名称: コンテンツ配信方法およびコンテンツ配信システム



16...MOBILE APPARATUS
15...MOBILE PACKET COMMUNICATION NETWORK
17...GATEWAY SERVER APPARATUS
18...MANAGEMENT SERVER APPARATUS
200...LIST FILE
12...IP SERVER APPARATUS
211...EXPLANATION FILE
207...EXPLANATION FILE
214...Jar FILE
210...Jar FILE
11...INTERNET
13...IP SERVER APPARATUS
202...EXPLANATION FILE
206...Jar FILE
14...IP SERVER APPARATUS

(57) Abstract: A mobile apparatus (16) capable of activating Java-AP software receives SDF (Security Description File)(204) from a management server apparatus (18) managed by a reliable organization (a communication business entity managing a mobile packet communication network 15); obtains ADF (205) from an IP server apparatus (13) by use of a URL included in the SDF; obtains a Jar file (206) from the IP server apparatus (13) by use of the ADF (205); and installs into itself Java-AP software including these files. The Java-AP, which is realized by activating the Java-AP software, operates within the range of the right represented by policy information included in the SDF (204).

[続葉有]

WO 03/058411 A1

丁目１１番１号山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP). 川端博史 (KAWABATA,Hiroshi) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目１１番１号山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP). 近藤隆 (KONDO,Takashi) [JP/JP]; 〒100-6150 東京都千代田区永田町二丁目１１番１号山王パークタワー株式会社エヌ・ティ・ティ・ドコモ知的財産部内 Tokyo (JP).

(74) 代理人: 川崎研二 (KAWASAKI,Kenji); 〒103-0027 東京都中央区日本橋一丁目２番１０号東洋ビルディング７階朝日特許事務所 Tokyo (JP).

(81) 指定国 (国内): AU, BR, CA, CN, ID, IN, KR, NO, NZ, PH, PL, SG, US.

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

Ｊａｖａ－ＡＰソフトウェアを起動することができる移動機１６が、信頼できる機関（移動パケット通信網１５を管理する通信事業者）が管理する管理サーバ装置１８からＳＤＦ（セキュリティ記述ファイル）２０４を受信し、このＳＤＦに内包されているＵＲＬを用いてＩＰサーバ装置１３からＡＤＦ２０５を取得し、このＡＤＦ２０５を用いてＩＰサーバ装置１３からＪａｒファイル２０６を取得し、これらのファイルを内包するＪａｖａ－ＡＰソフトウェアを自身にインストールする。このＪａｖａ－ＡＰソフトウェアを起動することで実現されるＪａｖａ－ＡＰは、ＳＤＦ２０４に内包されているポリシー情報で表される権限の範囲内で動作する。

明細書

コンテンツ配信方法およびコンテンツ配信システム

技術分野

本発明は、端末装置にアプリケーションソフトウェアを配信する技術に関する。

背景技術

Ｊａｖａ（登録商標）プログラミング言語に従って記述されたプログラムを実行してＪａｖａ－ＡＰ（Ｊａｖａアプリケーション）を実行する機能と、この種のプログラムを含むＪａｖａ－ＡＰソフトウェアを、ネットワークを介してダウンロードする機能とを備えた移動機が普及している。

Ｊａｖａ－ＡＰソフトウェアとして、Ｊａｒ（Java Archive）ファイルとＡＤＦ（Application Descriptor File）とがある。ここで、Ｊａｒは、それが実行されることにより、あるＪａｖａ－ＡＰをユーザに提供するプログラムを内包している。また、ＡＤＦはＪａｒファイルに依存しており、例えば、Ｊａｒファイルの格納位置を示すＵＲＬ（以後、パッケージＵＲＬ）、Ｊａｒファイルのサイズを示す情報、Ｊａｒファイルの最終変更日時を示す情報等を必須情報として内包している。

移動機は、次のような手順で、所望のＪａｖａ－ＡＰに関連したソフトウェアのダウンロードを行う。まず、移動機は、ＷＷＷ（World Wide Web）を構成するサーバ装置から所望のＪａｖａ－ＡＰに関連したＡＤＦを取得する。

ＡＤＦを取得した移動機はこのＡＤＦの内容を調べ、所望のＪａｖａ

ーＡＰに関連したＪａｒファイルを当該移動機にインストール可能であるか否かを判断する。そして、インストール可能と判断すると、移動機は、ＡＤＦに含まれていたパッケージＵＲＬを用いて、ＷＷＷを構成するサーバ装置からＪａｒファイルを取得する。このＪａｒファイルの取得をもってＪａｖａーＡＰソフトウェアのダウンロードは完了する。その後、移動機においては、ダウンロードされたＪａｖａーＡＰソフトウェアのインストールが行われ、当該Ｊａｖａーソフトウェアは起動要求さえあれば実行される状態となる。

ところで、移動機内で実行されるＪａｖａーＡＰの挙動についての制限は、通信アプリケーションなどの移動機が元から備えているネイティブアプリケーションの挙動についての制限よりも厳しくなっている。例えば、Ｊａｖａーは、移動機内の電話番号データを参照することができないようになっている。このような厳しい制限を課すことにより、悪意をもって作成されたＪａｖａーＡＰ、あるいは不具合を有するＪａｖａーＡＰによって移動機内の秘密性の高い情報が漏洩したり改竄されたりする事態を確実に回避することができる。

しかし、上述した厳しい制限を全てのＪａｖａーＡＰに対して一律に課すだけでは、ユーザやＩＰ（情報提供事業者）の希望を満たすことはできない。例えば、ある程度の信頼性が保証されるのであれば、Ｊａｖａーに移動機に格納された個人情報を参照する権限を与えてもよいと感じるユーザがいると思われる。また、ＩＰにも、移動機に格納されている個人情報や移動機が有する多数の機能を使用するＪａｖａーＡＰを提供したいという希望がある。

これらの希望を満たすべく、移動機のユーザに対して通信サービスを提供する通信事業者等の信頼できる機関がＪａｖａーＡＰに権限を与え、この権限を移動機に通知し、当該権限に基づいて移動機が当該Ｊａｖａーの挙動を制限するという仕組みが考えられる。この仕組みでは、権限の信頼性を保証するために、信頼できる機関以外の他者が権限の付与・管理に関与し得ないようにすべきである。

Ｊａｖａ－ＡＰソフトウェアのダウンロード手順に上述の仕組みを適用する場合、ＡＤＦあるいはＪａｒファイルに権限を示す情報を内包させるのが妥当である。Ｊａｒファイルは ＩＰにより随時更新され、ＩＰが保有するのが適当であることから、信頼できる機関に保有させるならＡＤＦが権限を示す情報を内包させるのに妥当ということになる。

しかし、ＡＤＦはＪａｒファイルに依存した内容となることから、ＩＰが手元のＪａｒファイルを更新すると、信頼できる機関が保有しているＡＤＦの更新も必要になってくる。また、Ｊａｒファイルを更新せずとも、ＡＤＦの更新が必要となることがある。例えば、ＩＰにおいて、あるＪａｒファイルへのアクセスが殺到し、このＪａｒファイルを他のサーバ装置へ移動する場合である。この場合、Ｊａｒファイルの格納位置が変更されるから、ＡＤＦに内包されているパッケージＵＲＬを変更する必要がある。しかしながら、ＡＤＦは信頼できる機関において他者の関与を排するように管理されるのであるから、ＡＤＦの更新作業は繁雑な作業となると予想される。

発明の開示

本発明は、上述した事情に鑑みて為されたものであり、依存関係にある複数のファイルを配信することで配信される、アプリケーションを実現するためのソフトウェアを、ＩＰの自由度を制限することなく、権限に応じた挙動をアプリケーションに対して許可する端末装置へ配信する配信方法および配信システムを提供することを目的としている。

上述した課題を解決するために、本発明は、ファイルの格納位置を通知されると当該ファイルを返送する通信システムが、アプリケーションを実現するためのソフトウェアを内包した実体ファイルに依存した情報と前記実体ファイルの格納位置を示す情報とを含んだアプリケーション記述ファイルの格納位置を示す第１の識別情報と、前記ソフトウェアに従って実行されるアプリケーションの挙動の許容範囲に関する権限情報とを内包したセキュリティ記述ファイルを、当該ファイルを格納

した管理サーバ装置から前記セキュリティを確保して前記権限情報によって示された範囲内でアプリケーションの挙動を許可する端末装置へ送信する権限送信過程と、前記端末装置が、前記権限送信過程にて前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第１の識別情報を用いて、前記アプリケーション記述ファイルを記憶した１または複数のサーバ装置から、当該アプリケーション記述ファイルを取得する依存情報取得過程と、前記端末装置が、前記依存情報取得過程にて取得した前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得するプログラム取得過程とを有する配信方法を提供する。

この配信方法によれば、端末装置は、アプリケーションに対応したアプリケーション記述ファイルおよび実体ファイルを取得する前に、セキュリティが確保された上で通信システムから送信されるセキュリティ記述ファイルを取得する。このセキュリティ記述ファイルにはアプリケーションに与えられた権限が示されており、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。

また、本発明は、アプリケーションを実現するためのソフトウェアを内包した実体ファイルと、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルとを格納した１または複数のサーバ装置と、前記アプリケーション記述ファイルの格納位置を示す第１の識別情報と端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティー記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムと、アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、前記管理サーバ装置は、前記セキュリティ記述ファイルを前記端末装置へ、セキュリティを確保して送信し、前記端末装置は、前記通信システ

ムから送信された前記セキュリティ記述ファイルに内包されている前記第１の識別情報を用いて前記アプリケーション記述ファイルを取得し、前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する配信システムを提供する。

この配信システムによれば、端末装置は、アプリケーションに対応したアプリケーション記述ファイルおよび実体ファイルを取得する前に、セキュリティが確保された上で通信システムから送信されるセキュリティ記述ファイルを取得することになる。このセキュリティ記述ファイルにはアプリケーションに与えられた権限が示されており、端末装置では、取得したセキュリティ記述ファイルに示される権限に応じた挙動が当該セキュリティ記述ファイルに対応するアプリケーションに許可される。

図面の簡単な説明

図１は本発明の実施の一形態に係る配信システムの構成を示すブロック図である。

図２は同配信システムに特有のＡＤＦのデータ構成を示す概念図である。

図３は同配信システムを構成する移動機１６の構成を示すブロック図である。

図４は同移動機１６の機能構成を示す概念図である。

図５は同移動機１６がＪａｖａ－ＡＰソフトウェアをダウンロードしインストールする処理を示すフローチャートである。

図６は同配信システムにおいて管理サーバ装置１８に格納されているＳＤＦのデータ構成を示す概念図である。

図７は同ＳＤＦに内包されるポリシー情報の内容を示す概念図である。

図８は同配信システムの動作を説明するためのブロック図である。

図９は配信システムにて配信されるリストページを示す図である。

図１０は配信システムを構成するＩＰサーバ装置１２が格納している説明ファイルの内容を示す図である。

図１１は配信システムにて配信される説明ページを示す図である。

図１２はＩＰサーバ装置１２が格納している説明ファイルの内容を示す図である。

図１３は同配信システムにて配信される説明ページを示す図である。

図１４は同配信システムを構成するＩＰサーバ装置１３が格納している説明ファイルの内容を示す図である。

図１５は同配信システムにて配信される説明ページを示す図である。

図１６は同配信システムの動作を説明するためのシーケンス図である。

図１７は同配信システムの動作を説明するためのシーケンス図である。

図１８は同配信システムの動作を説明するためのシーケンス図である。

図１９は同配信システムの他の動作を説明するためのブロック図である。

図２０は同配信システムの他の動作を説明するためのシーケンス図である。

発明を実施するための最良の形態

以下、図面を参照して、本発明の実施の一形態である配信システムについて説明する。なお、図面において、共通する部分には同一の符号が付されている。

（１）構成

図１に示されるように、この配信システムにおいて、ＩＰサーバ装置１２～１４は、インターネット１１に接続されている。ＩＰサーバ装置１２は第１のＩＰ（Internet Provider）によって管理されており、ＩＰサーバ装置１３および１４は第１のＩＰと異なる第２のＩＰにより

管理されている。そして、ＩＰサーバ装置１２～１４はＷＷＷを構成しており、それぞれ一般的なＷＷＷサーバ装置と同様のハードウェアおよび機能を有する。移動パケット通信網１５は、通信事業者が移動パケット通信サービスを提供するために用いる網である。移動機１６は、この移動パケット通信網１５との間で無線パケット通信を行うことが可能である。ゲートウェイサーバ装置１７は、移動パケット通信網１５と同じ通信事業者により管理されている。このゲートウェイサーバ装置１７は、移動パケット通信網１５とインターネット１１とを接続する装置であり、一般的なゲートウェイサーバ装置の構成と同様の構成を有する。管理サーバ装置１８は、専用線によりゲートウェイサーバ装置１７に接続されている。この管理サーバ装置１８もまたＷＷＷを構成し、一般的なＷＷＷサーバ装置と同様のハードウェアおよび機能を有する。ゲートウェイサーバ装置１７は、移動パケット通信網１５とインターネット１１との間のパケット中継、管理サーバ装置１８と移動パケット通信網１５との間のパケット中継および管理サーバ装置１８とインターネット１１との間のパケット中継を行う。移動機１６は、この中継機能を利用することにより、移動パケット通信網１５およびインターネット１１を介してＩＰサーバ装置１２～１４とパケット通信を行うことが可能である。なお、実際の配信システムには多数の移動機が存在するが、図面が繁雑になるのを避けるために一つの移動機１６のみが図示されている。これと同様の理由により、３つのＩＰサーバ装置１２～１４のみが図示されている。

この配信システムにおいて、移動機１６は、インターネット１１上の所望のサイトからＪａｖａ－ＡＰソフトウェアを受け取ることができる。この移動機１６が受け取ることができるソフトウェアは、トラステッドＪａｖａ－ＡＰに関するものと、非トラステッドＪａｖａ－ＡＰに関するものに大別される。ここで、トラステッドＪａｖａ－ＡＰソフトウェアは、移動パケット通信網１５を管理する通信事業者が、ＩＰサーバ装置１２～１４を管理するＩＰとの契約に基づいて信頼性を保証し

たＪａｖａ－ＡＰソフトウェアである。また、非トラステッドＪａｖａ－ＡＰソフトウェアは、トラステッドＪａｖａ－ＡＰソフトウェア以外のＪａｖａ－ＡＰソフトウェアである。

管理サーバ装置１８は、この配信システム内を流通する各トラステッドＪａｖａ－ＡＰソフトウェアについてＳＤＦ（セキュリティ記述ファイル）を各々記憶している。このＳＤＦは、移動パケット通信網１５を管理する通信事業者によって作成されるファイルであり、移動機のトラステッドＡＰＩ（APplication Interface）を使用するＪａｖａ－ＡＰソフトウェアを移動機にダウンロードする際に必須のファイルである。なお、トラステッドＡＰＩについては後述する。図６に示されるように、ＳＤＦは、トラステッドＪａｖａ－ＡＰソフトウェアを識別するためのＡＰＩＤ、ポリシー情報、当該Ｊａｖａ－ＡＰソフトウェアに対応したＡＤＦの記憶位置を示すＡＤＦ－ＵＲＬ、および当該Ｊａｖａ－ＡＰソフトウェアを提供するＩＰに対してＣＡが付与した公開鍵を有する。ここで、ポリシー情報は、Ｊａｖａ－ＡＰの挙動に対する制限を示す情報である。なお、このポリシー情報およびこれに基づいて行われるＪａｖａ－ＡＰの挙動の制限の詳細については後述する。

本実施形態では、移動機１６からの要求により、ＩＰサーバ装置１２～１４の１つから移動機１６にトラステッドＪａｖａ－ＡＰソフトウェアが配信される場合に、これに対応したＳＤＦが管理サーバ装置１８から移動機１６に配信される。そして、移動機１６において、トラステッドＪａｖａ－ＡＰソフトウェアが実行されるときには、これに対応したＳＤＦに基づいて、トラステッドＪａｖａ－ＡＰの挙動の制限が行われる。これが本実施形態の特徴の１つである。図１に示すとおり、ＳＤＦの送信は移動パケット通信網１５を通して行われ、管理サーバ装置１８とゲートウェイサーバ装置１７は専用線によって接続されている。また、送信に際し、ＳＤＦは暗号化される。

以下、この特徴との関連において、配信システムの各要素の構成を説明する。

ＩＰサーバ装置１２、１３及び１４は不揮発性メモリ１２Ａ，１３Ａ及び１４Ａをそれぞれ有する。

不揮発性メモリ１２Ａ、１３Ａおよび１４Ａは、ハードディスク等の不揮発性メモリであり、Ｊａｒファイルおよびａｄｆからなるｊａｖａ－ＡＰソフトウェアと、ｊａｖａ－ＡＰソフトウェアの内容を移動機のユーザに説明するための説明ファイルとを記憶している。

不揮発性メモリ１２Ａ、１３Ａおよび１４Ａに記憶されている個々のｊａｖａ－ＡＰソフトウェアは、トラステッドｊａｖａ－ＡＰソフトウェアであるかも知れないし、非トラステッドｊａｖａ－ＡＰソフトウェアであるかも知れない。トラステッドｊａｖａ－ＡＰであるか非トラステッドｊａｖａ－ＡＰであるかに拘わらず、全てのｊａｖａ－ＡＰソフトウェアのａｄｆには、ＷＷＷにおけるＪａｒファイルの記憶位置を示すパッケージＵＲＬや、Ｊａｒファイルのサイズを示す情報、Ｊａｒファイルの最終変更日時を示す情報等が記述されている。これらはｊａｖａ－ＡＰソフトウェアのａｄｆに記述されるべき項目として一般的に知られているものである。そして、トラステッドｊａｖａ－ＡＰソフトウェアのａｄｆは、これらの一般的に知られた情報の他に、図２に示されるように、そのトラステッドｊａｖａ－ＡＰソフトウェアのＡＰＩＤとＪａｒファイルのハッシュ値とを内包している。さらにトラステッドｊａｖａ－ＡＰソフトウェアのａｄｆは、当該ソフトウェアを提供するＩＰに対してＣＡ（認証局）から付与された秘密鍵で暗号化されている。

また、説明ファイルは、ＨＴＭＬに従って記述されたテキストファイルである。移動機は、あるｊａｖａ－ＡＰソフトウェアをダウンロードする場合に、それに先だって、このｊａｖａ－ＡＰソフトウェアに対応した説明ファイルをダウンロードする必要がある。説明ファイルには、ｊａｖａ－ＡＰソフトウェアのダウンロードの指示をユーザから受け取るＵＩ（ユーザインターフェイス）を構成するための情報が含まれている。移動機１６は、この情報に従い、ＵＩ画面を表示する。ユーザは、このＵＩ画面中の所望のｊａｖａ－ＡＰを表すオブジェクトを指定す

る操作を移動機１６に対して行うことができる。説明ファイルには、このようにしてユーザによって指定されるオブジェクトを、ダウンロード対象であるＪａｖａ－ＡＰソフトウェアに対応するＳＤＦ（ＳＤＦが存在しない場合にはＡＤＦ）のWWWにおける所在を示すＵＲＬに対応付けるように記述されている。

ＩＰサーバ装置１２～１４の各々は、以上説明した各ファイルをＩＰの指示に従って作成および更新する機能を備えている。

管理サーバ装置１８は、ハードディスク等の不揮発性メモリ１８Ａを有する。管理サーバ装置１８は、ＴＣＰコネクションを通信相手との間に確立する。管理サーバ装置１８は、このTCPコネクションを介して、ＨＴＴＰのＧＥＴメソッドを用いた要求メッセージを通信相手から受信すると、当該ＧＥＴメソッドに指定されたＵＲＬで特定されるファイルを不揮発性メモリ１８Ａから読み出し、このファイルを含むＨＴＴＰの応答メッセージを返送して当該コネクションを切断する。

また、上記不揮発性メモリ１８Ａには、ダウンロード可能なＪａｖａ－ＡＰソフトウェアを移動機１６のユーザに紹介するためのリストファイル２００と、このリストファイル２００に挙げられた各Ｊａｖａ－ＡＰソフトウェアに各々対応したＳＤＦとが記憶される。

リストファイル２００は、ＳＤＦと同様、ＩＰサーバ装置１３～１５を管理する各ＩＰと管理サーバ装置１８を管理する通信事業者との間で結ばれた契約に従って通信事業者により作成されたファイルである。このリストファイル２００はＨＴＭＬに従って記述されたテキストファイルである。既に説明したように、移動機は、あるＪａｖａ－ＡＰソフトウェアのＳＤＦをダウンロードする場合に、そのＳＤＦのＵＲＬを含む説明ファイルを取得する必要がある。移動機１６は、この説明ファイルを格納しているＩＰサーバ装置にアクセスするという方法により、この説明ファイルを取得することができる。しかし、このような直接的な方法以外に、本実施形態において移動機１６は、次のような手順により所望のＪａｖａ－ＡＰソフトウェアの説明ファイルを取得すること

もできる。まず、移動機１６は、管理サーバ装置１８にアクセスして、このリストファイル２０を取得し、これに従い、ＵＩ画面を表示する。ユーザは、このＵＩ画面中の所望のＪａｖａ－ＡＰを表すオブジェクトを指定する操作を移動機１６に対して行うことができる。リストファイル２００は、このようにしてユーザによって指定されるオブジェクトを、ダウンロード対象であるＪａｖａ－ＡＰソフトウェアの説明ファイルのWWWにおける所在を示すＵＲＬに対応付ける。移動機１６は、このようにリストファイル２００を介して得られるＵＲＬを用いて、ＩＰサーバ装置から説明ファイルを取得するのである。

移動機１６は、図３に示されるように、ＯＳ（オペレーティングシステム）ソフトウェア、Ｊａｖａ－ＡＰを実行する環境を構築するためのＪａｖａ－ＡＰ環境ソフトウェアおよび各種ネイティブＡＰソフトウェア等を記憶したＲＯＭ１６Ａと、ＲＯＭ１６Ａに接続されＲＯＭ１６Ａからプログラムを読み出して実行するＣＰＵ１６Ｂと、ＣＰＵ１６Ｂに接続された表示部１６Ｃと、不揮発性メモリ１６Ｄと、ＲＡＭ１６Ｅと、通信部１６Ｆと、操作部１６Ｇとを有する。

表示部１６Ｃは、例えば液晶表示パネルを有し、ＣＰＵ１６Ｂから供給されるデータを画像として表示する。不揮発性メモリ１６Ｄは例えばＳＲＡＭやＥＥＰＲＯＭであり、ＣＰＵ１６Ｂによりデータを読み書きされる。不揮発性メモリ１６Ｄは、WWWを構成するサーバ装置（以後、Ｗｅｂサーバ装置）からダウンロードしたＪａｖａ－ＡＰソフトウェア（ＡＤＦおよびＪａｒ）や、ＳＤＦを記憶するために使用される。

通信部１６Ｆは、移動パケット通信網１５と無線パケット通信を行うものであり、ＣＰＵ１６Ｂと移動パケット通信網１５との間でパケットを中継する。また、通信部１６Ｆは、アンテナや無線送受信部の他に、通話のためのＣＯＤＥＣやマイク、スピーカ等を備えている。従って、移動機１６は、この通信部１６Ｆにより、図示せぬ移動通信網を介して回線交換による通話を行うこともできる。操作部１６Ｇは操作子を備え、操作子の操作に応じた信号をＣＰＵ１６Ｂへ供給する。

図示せぬ電源が投入されると、ＣＰＵ１６ＢはＲＡＭ１６Ｅをワークエリアとし、ＲＯＭ１６ＡからＯＳソフトウェアに内包されているプログラムを読み出して実行する。これにより、ＣＰＵ１６ＢにはＵＩ等を提供する機能が実行される。すなわち、ＣＰＵ１６ＢはＯＳソフトウェアを起動して移動機１６内にて図４のＯＳを実行する。ＯＳは操作部１６Ｇから供給される信号とＵＩの状態とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。

ユーザの指示がネイティブＡＰソフトウェアである通信ソフトウェアの起動を要求するものであれば、ＯＳは通信ソフトウェアを起動して移動機１６内にて通信ＡＰを実行する。この通信ＡＰを用いることで、ユーザは通話相手と通話をすることができる。

ユーザの指示がネイティブＡＰソフトウェアである電話帳ＡＰの起動を要求するものであれば、ＯＳは電話帳ソフトウェアを起動して移動機１６内にて電話帳ＡＰを実行する。この電話帳ＡＰを用いることで、ユーザは、不揮発性メモリ１６Ｄに記憶された電話帳の内容（以後、電話帳データ）を参照・使用・変更することができる。

ユーザの指示がネイティブＡＰソフトウェアであるＷｅｂブラウザソフトウェアの起動を要求するものであれば、ＯＳはＷｅｂブラウザソフトウェアを起動して移動機１６内にてＷｅｂブラウザを実行する。また、ＷｅｂブラウザはＵＩを提供する。そして、ユーザから操作部１６Ｇの操作により指示があると、ＵＩの状態と操作部１６Ｇから供給される信号とに基づいてユーザの指示を特定し、この指示に応じた処理を行う。例えば、当該指示が指定されたファイルをＷＷＷから取得する旨の場合には、通信部１６Ｆを制御して当該ファイルを記憶したＷｅｂサーバ装置との間にＴＣＰコネクションを確立し、このコネクションを介して、指定された位置を示すＵＲＬでＧＥＴメソッドを用いたＨＴＴＰの要求メッセージを送信し、この要求メッセージに対応する応答メッセージを受信し、当該コネクションを切断する。さらに、Ｗｅｂブラウザは、受信した応答メッセージに内包されているファイルをＨＴＭＬに従っ

て解釈し、Ｗｅｂページを内包するＵＩを生成し、ユーザに提供する。また、ユーザの指示がＪａｖａ－ＡＰソフトウェアのダウンロードを要求するものである場合には、この指示を次に述べるＪＡＭ（Java Application Manager）に通知する。具体的には、Ｗｅｂページにおいて、クリック操作またはプレス操作により、オブジェクトタグが指定されているアンカータグで表されるアンカーが指定されると、Ｗｅｂブラウザは当該オブジェクトタグのｄａｔａ属性に指定されているＵＲＬを抽出し、当該ＵＲＬからのＪａｖａ－ＡＰソフトウェアのダウンロードが要求されたことをＪＡＭに通知する。

ユーザの指示がネイティブＡＰソフトウェアであるＪＡＭソフトウェアの起動を要求するものであれば、ＯＳはＪＡＭソフトウェアを起動して移動機１６内にてＪＡＭを実行する。ＪＡＭは、移動機１６にインストールされているＪａｖａ－ＡＰソフトウェアの一覧をユーザに提示し、ユーザにより指定されたＪａｖａ－ＡＰソフトウェアを起動する。具体的には、ＪＡＭに対するユーザの指示がＪａｖａ－ＡＰソフトウェアの起動を要求するものであれば、Ｊａｖａ－ＡＰ環境ソフトウェアが起動されて移動機１６内にＪａｖａ－ＡＰ環境が実行される。そして、指定されたＪａｖａ－ＡＰソフトウェアが起動されてＪａｖａ－ＡＰ環境内にＪａｖａ－ＡＰが実行される。Ｊａｖａ－ＡＰ環境は、携帯端末に適した軽量のＪａｖａ仮想マシンであるＫＶＭと、Ｊａｖａ－ＡＰに対して提供されるＡＰＩとを有する。Ｊａｖａ－ＡＰに対して提供されるＡＰＩは、通信事業者がＩＰとの契約に基づいて信頼性を保証したＪａｖａ－ＡＰ（以後、トラステッドＡＰ）のみに使用が許可されるトラステッドＡＰＩと、あらゆるＪａｖａ－ＡＰに使用が許可される非トラステッドＡＰＩとに分けられる。

（２）動作

以下、本実施形態の動作を説明する。ＪＡＭは、Ｊａｖａ－ＡＰのダウンロードを要求する指示がＷｅｂブラウザから通知されると、Ｊａｖａ－ＡＰソフトウェアを移動機１６にダウンロードしインストールす

る処理を行う。この処理の流れを図５に示す。なお、図５では、移動機１６が説明ファイルを取得するまでの過程は省略されている。説明ファイルの取得までの過程は、幾つかの態様があるので、後に具体的な動作例を挙げて説明する。図５に示されるように、ＪＡＭは、まず、ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＪａｖａ－ＡＰソフトウェアであるか否かを判定する（ステップＳ１１）。具体的には、移動機１６が説明ファイルを取得すると、Ｗｅｂブラウザは、この説明ファイルに応じたＵＩをユーザに提供し、Ｊａｖａ－ＡＰソフトウェアのダウンロードに関するユーザからの指示を受け取る。Ｗｅｂブラウザは、このユーザからの指示により特定されたＪａｖａ－ＡＰソフトウェアのＵＲＬをＪＡＭに通知する。ＪＡＭは、Ｗｅｂブラウザから通知されたＵＲＬの末尾のファイル名を参照し、このファイルの拡張子が“sdf”であればトラステッドＪａｖａ－ＡＰソフトウェア“sdf”でなければ非トラステッドＪａｖａ－ＡＰソフトウェアであると判定する。ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＪａｖａ－ＡＰソフトウェアであると判定された場合には、従来と同様のダウンロードおよびインストール処理が行われる（ステップＳ１２）。

ダウンロードしようとするＪａｖａ－ＡＰソフトウェアがトラステッドＪａｖａ－ＡＰソフトウェアと判定された場合には、ＪＡＭは、当該ソフトウェアに対応するＳＤＦを管理サーバ装置１８から取得する（ステップＳ１３）。すなわち、ＪＡＭは、管理サーバ装置１８との間にＴＣＰコネクションを確立し、このコネクションを介して、Ｗｅｂブラウザから通知されたＵＲＬで示される位置に記憶されたＳＤＦの送信を管理サーバ装置１８に要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、上記コネクションを切断する。

そして、ＪＡＭは、応答メッセージに内包されているＳＤＦからＡＰＩＤとＡＤＦ－ＵＲＬと公開鍵を抽出するとともに、当該ＳＤＦを不揮

発性メモリ１６Ｄに書き込む。

次に、ＪＡＭはＡＤＦを取得する（ステップＳ１４）。具体的には、ＪＡＭは、ＳＤＦから抽出したＡＤＦ－ＵＲＬで特定されるＡＤＦを記憶したＷｅｂサーバ装置との間にＴＣＰコネクションを確立し、当該ＡＤＦの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、当該ＴＣＰコネクションを切断する。

既に説明したように、トラステッドＪａｖａ－ＡＰソフトウェアに対応するＡＤＦは、ＡＰＩＤとＪａｒファイルのハッシュ値とを内包し、さらに当該トラステッドＪａｖａ－ＡＰソフトウェアを提供するＩＰに対してＣＡが付与した秘密鍵により署名（暗号化）されている。そこで、ＪＡＭは、応答メッセージに内包されているＡＤＦの署名をＳＤＦから抽出された公開鍵を用いて検証し（復号し）、当該ＡＤＦの正当性を判断する（ステップＳ１５）。

ＡＤＦが正当であると判断した場合には、ＪＡＭは、ＳＤＦから抽出したＡＰＩＤとＡＤＦに内包されているＡＰＩＤとを比較し、両者が一致するか否かを判定する（ステップＳ１６）。両者が一致すると判定された場合には、ＪＡＭは、当該トラステッドＪａｖａ－ＡＰソフトウェアを移動機１６にインストール可能か否かをＡＤＦの内容に基づいて判定する（ステップＳ１７）。この判定の基準は従来と同様である。

インストール可能と判定された場合には、ＪＡＭは、Ｊａｒファイルを取得する。具体的には、ＪＡＭは、当該ＡＤＦを移動機１６に書き込むとともに、当該ＡＤＦからハッシュ値とパッケージＵＲＬを抽出する。さらにＪＡＭは、このパッケージＵＲＬで特定されるＪａｒファイルを記憶したＷｅｂサーバ装置との間にＴＣＰコネクションを確立し、当該Ｊａｒファイルの送信を要求する内容の要求メッセージを生成・送信し、このメッセージに対する応答メッセージを受信し、当該ＴＣＰコネクションを切断する（ステップＳ１８）。

さらに、ＪＡＭは、取得したＪａｒファイルに対するハッシュ値を算

出する（ステップＳ１９）。ハッシュ値の算出に使用するハッシュ関数は任意であるが、移動機で使用されるハッシュ関数とＡＤＦに含まれるハッシュ値を算出するためにＩＰが用いるハッシュ関数は一致していなければならない。

ＪＡＭは、ＪＡＭが算出したハッシュ値とＡＤＦから抽出したハッシュ値とを比較し（ステップＳ２０）、両者が一致した場合には、取得したＪａｒファイルを管理サーバ装置１８に書き込み、トラステッドＪａｖａ－ＡＰソフトウェアのインストールに係る各種処理を行い（ステップＳ２１）、インストールに成功した旨をユーザに通知する（ステップＳ２２）。

ＡＤＦが正当でないと判断した場合、ＳＤＦが有するＡＰＩＤとＡＤＦが有するＡＰＩＤが不一致の場合、インストールしようとするＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断した場合、算出したハッシュ値とＡＤＦが有するハッシュ値とが不一致の場合には、ＪＡＭは、インストールに失敗した旨をユーザに通知するとともに、移動機１６の状態を、ＳＤＦの取得を開始する前の状態に戻す。

また、ＪＡＭは、Ｊａｖａ－ＡＰの挙動を監視し、トラステッドＡＰＩの使用を制限する。この制限は不揮発性メモリ１６Ｄに記憶されるＳＤＦ内のポリシー情報に従って行われる。ＳＤＦ内のポリシー情報は、例えば図７に概念的に示されるような内容となっている。図７に示されるポリシー情報では、移動機に格納された電話帳データを参照するときに必須のトラステッドＡＰＩである“getPhoneList()”と移動機の状態を取得するときに必須のトラステッドＡＰＩである“getMsStatus()”の使用が許可され、移動機に格納された発着信履歴データを参照するときに必須のトラステッドＡＰＩである“getCallHistory()”の使用が禁止されている。

（３）具体的動作例

次に、上述したシステムの動作例について説明する。

なお、以下に述べる動作において、ＴＣＰコネクションの確立および

切断動作についてはＨＴＴＰにおける一般的な動作となることから、それらの説明を省略する。また、前述のＯＳ、Ｗｅｂブラウザ、ＪＡＭ、Ｊａｖａ－ＡＰ、ネイティブＡＰ等が行う動作は移動機１６の動作となることから、以降の説明では、動作の主体を移動機１６とする。

以下説明する動作例では、次のような状況を想定している。まず、図８に示されるように、管理サーバ装置１８の不揮発性メモリ１８Ａには、リストファイル２００とＳＤＦ２０４が記憶されている。ここで、リストファイル２００は、移動機１６において解釈・実行されると図９に示されるリストページ２０１を提供するように記述されている。また、リストファイル２００は、クリックまたはプレス操作により、リストページ２０１を構成する選択肢２０１Ａが指定されると、説明ファイル２０２のＵＲＬ（“http://www.main.bbb.co.jp/ghi.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。さらに、リストファイル２００は、リストページ２０１を構成する選択肢２０１Ｂが指定されると、説明ファイル２０７のＵＲＬ（“http://www.ccc.co.jp/jkl.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージが生成されるように記述されている。

また、ＳＤＦ２０４は、ＡＰＩＤとして“0001”、ポリシー情報として図７に示される情報、ＡＤＦ－ＵＲＬとして“http://www.main.bbb.co.jp/viewer.jam”、およびＩＰサーバ装置１３とＩＰサーバ装置１４を管理するＩＰに対してＣＡが付与した公開鍵を内包している。

また、ＩＰサーバ装置１２の不揮発性メモリ１２Ａには、「詰め将棋」(西洋社会における「チェスパズル」に類似するゲーム)なる名称のＪａｖａ－ＡＰソフトウェア（以後、第１のＪａｖａ－ＡＰソフトウェア）に対応する説明ファイル２１１、ＡＤＦ２１３およびＪａｒファイル２１４が記憶されている。説明ファイル２１１、ＡＤＦ２１３およびＪａｒファイル２１４はＩＰサーバ装置１２を管理するＩＰによって作成されている。説明ファイル２１１の内容は図１０に示される通りである。説明ファイル２１１は、移動機１６において解釈・実行されると図１１

に示される説明ページ２１２を提供するように記述されている。また、ＡＤＦ２１３はパッケージＵＲＬとしてＪａｒファイル２１４のＵＲＬ（“http://www.ccc.co.jp/shogi.jar”）を内包している。

また、ＩＰサーバ装置１２の不揮発性メモリ１２Ａには、「星占い」なる名称のＪａｖａ－ＡＰソフトウェア（以後、第２のＪａｖａ－ＡＰソフトウェア）に対応する説明ファイル２０７、ＡＤＦ２０９およびＪａｒファイル２１０が記憶されているものとする。説明ファイル２０７、ＡＤＦ２０９およびＪａｒファイル２１０はＩＰサーバ装置１２を管理するＩＰによって作成されている。説明ファイル２０７の内容は図１２に示される通りである。説明ファイル２０７は、移動機１６において解釈・実行されると図１３に示される説明ページ２０８を提供するように記述されている。また、ＡＤＦ２０９はパッケージＵＲＬとしてＪａｒファイル２１０のＵＲＬ（“http://www.ccc.co.jp/horoscope.jar”）を内包している。

また、ＩＰサーバ装置１３の不揮発性メモリ１３Ａには、「電話帳ビューア」なる名称のＪａｖａ－ＡＰソフトウェア（以後、第３のＪａｖａ－ＡＰソフトウェア）に対応する説明ファイル２０２、ＡＤＦ２０５およびＪａｒファイル２０６が記憶されている。説明ファイル２０２、ＡＤＦ２０５およびＪａｒファイル２０６は、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰによって作成されている。説明ファイル２０２の内容は図１４に示される通りである。説明ファイル２０２は、移動機１６において解釈・実行されると図１５に示される説明ページ２０３を提供するように記述されている。ＡＤＦ２０５は、ＡＰＩＤとして“0001”、Ｊａｒファイル２０６のハッシュ値、パッケージＵＲＬとしてＪａｒファイル２０６のＵＲＬ（“http://www.main.bbb.co.jp/viewer.jar”）を内包しており、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰに対してＣＡが付与した秘密鍵を用いて署名されている。

また、移動機１６は第１～第３のＪａｖａ－ＡＰソフトウェアをイン

ストール可能な状態にある。

（２－１）インストール動作

まず、ＪａｖａーＡＰソフトウェアを移動機１６にインストールする場合の動作例について、ＪａｖａーＡＰソフトウェア毎に説明する。

（２－１－１）第１のＪａｖａーＡＰソフトウェア

第１のＪａｖａーＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、Ｗｅｂブラウザにより、所望のＪａｖａーＡＰソフトウェアを格納しているＩＰサーバ装置を求め、そこから説明ファイル２１１の取得を試みることから始まる。まず、移動機１６では、説明ファイル２１１のＵＲＬ（“http://www.ccc.co.jp/mno.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ１２が生成される。この要求メッセージｔｍ１２は、図１６に示されるように、移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ１２の内容に対応して説明ファイル２１１を内包した応答メッセージｔｍ１３が生成される。この応答メッセージｔｍ１３はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２１１の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１１に示すような説明ページ２１２が表示される。

この説明ページ２１２を視たユーザが、説明ページ２１２内のアンカー２１２Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１０の説明ファイル２１１に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）を特定する。そして、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.ccc.co.jp/shogi.jam”）が抽出され、図５におけるステップＳ１１の判断が行われる。この例では、ＵＲＬの拡張子がｓｄｆではないため、通常の処理（ステップＳ１２）が行われる。すなわち、次の通りである。まず、このＵＲＬで特定されるＡＤＦ２１３の送信を要求す

る内容の要求メッセージｔｍ１６が生成される。この要求メッセージｔｍ１６は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ１６の内容に対応してＡＤＦ２１３を内包した応答メッセージｔｍ１７が生成される。この応答メッセージｔｍ１７はＩＰサーバ装置１２から送信され移動機１６により受信される。

移動機１６では、ＡＤＦ２１３の内容に基づいて第１のＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動機１６は第１のＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では第１のＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

次に、移動機１６では、ＡＤＦ２１３が不揮発性メモリ１６Ｄ１に書き込まれる。また、移動機１６では、ＡＤＦ２１３からパッケージＵＲＬ（“http://www.ccc.co.jp/shogi.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２１４の送信を要求する内容の要求メッセージｔｍ１８が生成される。この要求メッセージｔｍ１８は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ１８の内容に対応してＪａｒファイル２１４を内包した応答メッセージｔｍ１９が生成される。この応答メッセージｔｍ１９はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６ではＪａｒファイル２１４が不揮発性メモリ１６Ｄ１に書き込まれ、第１のＪａｖａ－ＡＰソフトウェアのインストールが完了する。

なお、移動機１６において第１のＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、移動機１６の状態は、ＡＤＦ２１３の取得を開始する前の状態に戻る。

（２－１－２）第２のＪａｖａ－ＡＰソフトウェア

第２のＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２０７の取得を試みることから始ま

る。既に説明したように、説明ファイル２０７は、関連するＩＰサーバ装置への直接アクセスまたはリストファイル２００経由のいずれかにより取得可能であるが、ここでは、リストファイル２００の取得を試みることから始まる動作のみについて説明する。

図１７に示されるように、移動機１６では、リストファイル２００のＵＲＬ（“http://www.aaa.co.jp/def.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ２０が生成される。この要求メッセージｔｍ２０は移動機１６から送信され管理サーバ装置１８により受信される。管理サーバ装置１８では、この要求メッセージｔｍ２０の内容に対応してリストファイル２００を内包した応答メッセージｔｍ２１が生成される。この応答メッセージｔｍ２１は管理サーバ装置１８から送信され移動機１６により受信される。移動機１６では、応答メッセージｔｍ２１の受信を契機として、応答メッセージｔｍ２１内のリストファイル２００がＨＴＭＬに従って解釈され、移動機１６のユーザに対して、リストファイル２００の内容に応じたＵＩが提供される。この結果、移動機１６の表示部１６Ｃには、例えば図９に示すようなリストページ２０１が表示される。

このリストページ２０１を視たユーザが、リストページ２０１内の選択肢２０１Ｂが押下されるように移動機１６を操作すると、移動機１６では、選択肢２０１Ｂに対応付けられているＵＲＬ（“http://www.ccc.co.jp/jkl.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ２２が生成される。この要求メッセージｔｍ２２は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ２２の内容に対応して説明ファイル２０７を内包した応答メッセージｔｍ２３が生成される。この応答メッセージｔｍ２３はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２０７の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１３に示すような説明ページ２０８が表示される。

この説明ページ２０８を視たユーザが、説明ページ２０８内のアンカー２０８Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１２の説明ファイル２０７に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）を特定する。そして、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http://www.ccc.co.jp/horoscope.jam”）が抽出され、図５におけるステップＳ１１の判断を行が行われる。この例では、ＵＲＬの拡張子がｓｄｆではないため、通常の処理（ステップＳ１２）が行われる。すなわち、次の通りである。まず、このＵＲＬで特定されるＡＤＦ２０９の送信を要求する内容の要求メッセージｔｍ２６が生成される。この要求メッセージｔｍ２６は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ２６の内容に対応してＡＤＦ２０９を内包した応答メッセージｔｍ２７が生成される。この応答メッセージｔｍ２７はＩＰサーバ装置１２から送信され移動機１６により受信される。

移動機１６では、ＡＤＦ２０９の内容に基づいて第２のＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される。前述のように、移動機１６は第２のＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では第２のＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

次に、移動機１６では、ＡＤＦ２０９が不揮発性メモリ１６Ｄ１に書き込まれる。また、移動機１６では、ＡＤＦ２０９からパッケージＵＲＬ（“http://www.ccc.co.jp/horoscope.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２１０の送信を要求する内容の要求メッセージｔｍ２８が生成される。この要求メッセージｔｍ２８は移動機１６から送信されＩＰサーバ装置１２により受信される。ＩＰサーバ装置１２では、この要求メッセージｔｍ２８の内容に対応してＪａｒファイル２１０を内包した応答メッセージｔｍ２９が生成され

る。この応答メッセージｔｍ２９はＩＰサーバ装置１２から送信され移動機１６により受信される。移動機１６ではＪａｒファイル２１０が不揮発性メモリ１６Ｄ１に書き込まれ、第２のＪａｖａ－ＡＰソフトウェアのインストールが完了する。

なお、移動機１６において、第２のＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、移動機１６の状態は、ＡＤＦ２０９の取得を開始する前の状態に戻る。

（２－１－３）第３のＪａｖａ－ＡＰソフトウェア

第３のＪａｖａ－ＡＰソフトウェアのインストール動作は、ユーザが移動機１６を操作し、説明ファイル２０２の取得を試みることから始まる。この動作例において、移動機１６は関連するリストファイル２００を取得して、説明ファイル２０２の所在を求め、説明ファイル２０２の取得を試みる。

図１８に示されるように、リストファイル２００の取得を試みることから始まる動作において、移動機１６が応答メッセージｔｍ２１を受信し、例えば図９に示すようなリストページ２０１が表示されるまでは図１７に示す動作と同一の動作が行われる。このリストページ２０１を視たユーザが、リストページ２０１内の選択肢２０１Ａが押下されるように移動機１６を操作すると、移動機１６では、選択肢２０１Ａに対応付けられているＵＲＬ（“http://www.main.bbb.co.jp/ghi.html”）をＧＥＴメソッドのパラメータとして含む要求メッセージｔｍ３２が生成される。この要求メッセージｔｍ３２は移動機１６から送信されＩＰサーバ装置１３により受信される。ＩＰサーバ装置１３では、この要求メッセージｔｍ３２の内容に対応して説明ファイル２０２を内包した応答メッセージｔｍ３３が生成される。この応答メッセージｔｍ３３はＩＰサーバ装置１３から送信され移動機１６により受信される。移動機１６では、ユーザに対して、説明ファイル２０２の内容に応じたＵＩが提供される。この結果、表示部１６Ｃには、例えば図１５に示すような説明ページ２０３が表示される。

この説明ページ２０３を視たユーザが、説明ページ２０３内のアンカー２０３Ａが押下されるよう移動機１６を操作すると、移動機１６では、図１４の説明ファイル２０２に記述されたアンカータグ（“<A”で始まるタグ）のｉｊａｍ属性に指定されている値がｉｄ属性に指定されているオブジェクトタグ（“<OBJECT”で始まるタグ）を特定する。そして、このオブジェクトタグのｄａｔａ属性に指定されているＵＲＬ（“http: //www.aaa.co.jp/abc.sdf”）が抽出され、図５におけるステップＳ１１の判断を行が行われる。この例では、ＵＲＬの拡張子がｓｄｆであるため、ステップＳ１３以降の処理が行われる。すなわち、次の通りである。まず、このＵＲＬで特定されるＳＤＦ２０４の送信を要求する内容の要求メッセージｔｍ３４が生成される。この要求メッセージｔｍ３４は移動機１６から送信され管理サーバ装置１８により受信される。管理サーバ装置１８では、この要求メッセージｔｍ３４の内容に対応してＳＤＦ２０４を内包した応答メッセージｔｍ３５が生成される。この応答メッセージｔｍ３５は管理サーバ装置１８から送信され、ゲートウェイサーバ装置１７及び移動パケット通信網１５を介して移動機１６により受信される。管理サーバ装置１８とゲートウェイサーバ装置１７との間の通信路は専用線であり、ゲートウェイサーバ装置１７はセキュリティの確保された移動パケット通信網１５に直接的に接続されていることから、移動機１６に受信されるまでにＳＤＦ２０４が改竄される虞は無い（以上、ステップＳ１３）。

移動機１６において、ＳＤＦ２０４は不揮発性メモリ１６Ｄの不揮発性メモリ１６Ｄ１に書き込まれる。また、移動機１６では、ＳＤＦ２０４からＡＰＩＤ（“0001”）とＡＤＦ－ＵＲＬ（“http://www.main.bbb.co.jp/viewer.jam”）と公開鍵が抽出され、このＡＤＦ－ＵＲＬで特定されるＡＤＦ２０５の送信を要求する内容の要求メッセージｔｍ３６が生成される。この要求メッセージｔｍ３６は移動機１６から送信されＩＰサーバ装置１３により受信される。ＩＰサーバ装置１３では、この要求メッセージｔｍ３６の内容に対応してＡＤＦ２０５を内包し

た応答メッセージｔｍ３７が生成される。この応答メッセージｔｍ３７はＩＰサーバ装置１３から送信され移動機１６により受信される（以上、ステップＳ１４）。

移動機１６ではＳＤＦ２０４から抽出された公開鍵を用いてＡＤＦ２０５の正当性が判断される（ステップＳ１５）。前述のように、ＳＤＦ２０４に内包されている公開鍵はＡＤＦ２０５への署名の際に用いた秘密鍵と対応していることから、ＩＰサーバ装置１３内あるいはＩＰサーバ装置１３から移動機１６への通信経路においてＡＤＦ２０５が変更されていない限り、ＡＤＦ２０５が正当であると判断される。

ＡＤＦ２０５が正当であると判断されると、移動機１６では、ＳＤＦ２０４から抽出されたＡＰＩＤとＡＤＦ２０５に内包されているＡＰＩＤとが比較される（ステップＳ１６）。前述のように、ＩＰサーバ装置１３におけるＡＤＦ２０５にはＳＤＦ２０４内のＡＰＩＤと一致するＡＰＩＤが記述されることから、記述ミス等が無い限り、ＳＤＦ２０４から抽出されたＡＰＩＤとＡＤＦ２０５に内包されているＡＰＩＤは一致する。

ＡＰＩＤが一致すると、移動機１６では、ＡＤＦ２０５の内容に基づいて第３のＪａｖａ－ＡＰソフトウェアをインストール可能か否かが判定される（ステップＳ１７）。前述のように、移動機１６は第３のＪａｖａ－ＡＰソフトウェアをインストール可能な状態にあるから、移動機１６では第３のＪａｖａ－ＡＰソフトウェアをインストール可能と判定される。

次に、移動機１６では、ＡＤＦ２０５が不揮発性メモリ１６Ｄ１に書き込まれる。また、移動機１６では、ＡＤＦ２０５からハッシュ値とパッケージＵＲＬ（“http://www.main.bbb.co.jp/viewer.jar”）が抽出され、このパッケージＵＲＬで特定されるＪａｒファイル２０６の送信を要求する内容の要求メッセージｔｍ３８が生成される。この要求メッセージｔｍ３８は移動機１６から送信されＩＰサーバ装置１３により受信される。ＩＰサーバ装置１３では、この要求メッセージｔｍ３８の

内容に対応してＪａｒファイル２０６を内包した応答メッセージｔｍ３９が生成される。この応答メッセージｔｍ３９はＩＰサーバ装置１３から送信され移動機１６により受信される（以上、ステップＳ１８）。

移動機１６ではＪａｒファイル２０６と所定のハッシュ関数とを用いてハッシュ値が算出され（ステップＳ１９）、この算出されたハッシュ値とＡＤＦ２０５から抽出されたハッシュ値とが比較される（ステップＳ２０）。前述のように、ＡＤＦ２０５には当該ＡＤＦ２０５に対応するＪａｒファイルのハッシュ値が記述されることから、記述ミス等がない限り、両ハッシュ値は一致する。両ハッシュ値が一致すると、移動機１６では、Ｊａｒファイル２０６が不揮発性メモリ１６Ｄ１に書き込まれ、第３のＪａｖａ－ＡＰソフトウェアのインストールが完了する（ステップＳ２１およびＳ２２）。

なお、移動機１６においてＡＤＦ２０５が正当でないと判断された場合や、ＳＤＦ２０４から抽出されたＡＰＩＤとＡＤＦ２０５に内包されているＡＰＩＤが不一致の場合、第３のＪａｖａ－ＡＰソフトウェアをインストール可能ではないと判断された場合、算出したハッシュ値とＡＤＦ２０５から抽出されたハッシュ値とが不一致の場合には、ユーザに対して失敗が通知され（ステップＳ２３）、移動機１６の状態は、ＳＤＦ２０４の取得を開始する前の状態に戻る。

（２－２）Ｊａｖａ－ＡＰソフトウェアが起動されている時の移動機１６の挙動

次に、Ｊａｖａ－ＡＰソフトウェアが起動されている時の移動機１６の挙動について説明する。

（２－２－１）第１のＪａｖａ－ＡＰソフトウェア

上述したインストール動作によりインストールされた第１のＪａｖａ－ＡＰソフトウェアが、ＪＡＭが実現された移動機１６において起動され、当該ソフトウェアに対応した機能（以後、第１のＪａｖａ－ＡＰ）が実現されたときの移動機１６の挙動について説明する。

第１のＪａｖａ－ＡＰが使用しようとするＡＰＩが非トラステッド

ＡＰＩの場合、当該ＡＰＩの使用はＪＡＭにより許可される。したがって、第１のＪａｖａ－ＡＰは当該ＡＰＩを使用することができる。

また、第１のＪａｖａ－ＡＰが使用しようとするＡＰＩがトラステッドＡＰＩの場合、ＪＡＭは当該Ｊａｖａ－ＡＰに対応するＳＤＦが不揮発性メモリ１６Ｄに記憶されているか否かを調べる。そのようなＳＤＦは不揮発性メモリ１６Ｄに記憶されていないから、ＪＡＭは第１のＪａｖａ－ＡＰによる当該ＡＰＩの使用を禁止する。したがって、第１のＪａｖａ－ＡＰは当該ＡＰＩの使用することができない。

（２－２－２）第２のＪａｖａ－ＡＰソフトウェア

インストールされた第２のＪａｖａ－ＡＰソフトウェアが、ＪＡＭが実現された移動機１６において起動され、当該ソフトウェアに対応した機能が実現されたときの移動機１６の挙動は、第１のＪａｖａ－ＡＰソフトウェアが起動されている時の移動機１６の挙動と同様となる。

（２－２－３）第３のＪａｖａ－ＡＰソフトウェア

インストールされた第３のＪａｖａ－ＡＰソフトウェアが、ＪＡＭが実現された移動機１６において起動され、当該ソフトウェアに対応した機能（以後、第３のＪａｖａ－ＡＰ）が実現されたときの移動機１６の挙動について説明する。

第３のＪａｖａ－ＡＰが使用しようとするＡＰＩが非トラステッドＡＰＩの場合当該ＡＰＩの使用はＪＡＭにより許可される。したがって、第３のＪａｖａ－ＡＰは当該ＡＰＩを使用することができる。

第３のＪａｖａ－ＡＰが使用しようとするＡＰＩがトラステッドＡＰＩの場合、移動機１６の挙動はＡＰＩに依存する。以下、ＡＰＩ毎に移動機１６の挙動を説明する。

（２－２－３－１）getPhoneList()

“getPhoneList()”はトラステッドＡＰＩであるから、当該ＡＰＩの使用の可否は、不揮発性メモリ１６Ｄに記憶されているＳＤＦ２０４内のポリシー情報に基づいてＪＡＭにより決定される。このポリシー情報の内容は図７に示される内容であることから、“getPhoneList()”の使

用がＪＡＭにより許可される。したがって、第３のＪａｖａ－ＡＰは“getPhoneList()”を使用することができる。つまり、第３のＪａｖａ－ＡＰは電話帳データを読み出すことができる。

（２－２－３－２）getCallHistory()

“getCallHistory()”はトラステッドＡＰＩであるから、当該ＡＰＩの使用の可否はＳＤＦ２０４内のポリシー情報に基づいてＪＡＭにより決定される。このポリシー情報の内容は図７に示される内容であることから、“getCallHistory()”の使用がＪＡＭにより禁止される。したがって、第３のＪａｖａ－ＡＰは“getCallHistory()”を使用することができない。つまり、第３のＪａｖａ－ＡＰは発着信履歴データを読み出すことができない。

（２－３）第３のＪａｖａ－ＡＰソフトウェアの変更後の動作

次に、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰが第３のＪａｖａ－ＡＰソフトウェアの配信形態や内容を変更した場合の本システム動作について説明する。ただし、ここでの変更は、第３のＪａｖａ－ＡＰソフトウェアの改善等を目的としたＪａｒファイル２０６の内容の変更と、ＩＰサーバ装置１３の負荷の軽減等を目的とした配信形態の変更とを含む。後者の変更を達成するために、ＩＰサーバ装置１３およびＩＰサーバ装置１４を管理するＩＰは、図１９に示すように、変更後のＪａｒファイル２０６（以後、Ｊａｒファイル２１５）をＩＰサーバ装置１４の不揮発性メモリ１４Ａに記憶させ、このＪａｒファイル２１５に対応するようにＡＤＦ２０５の内容を変更してＡＤＦ２１６としている。変更後の第３のＪａｖａ－ＡＰソフトウェアの配信に必要な作業は以上の通りであり、管理サーバ装置１８を管理する通信事業者が行うべき作業は存在しない。

このような変更の後の第３のＪａｖａ－ＡＰソフトウェアのインストール動作は、図２０に示す通りとなる。図２０に示す動作が図１８に示す動作と相違し始めるのは、ＩＰサーバ装置１３において、ＡＤＦ２０５を内包した応答メッセージｔｍ３７ではなく、ＡＤＦ２１６を内包

した応答メッセージｔｍ４７を生成してからである。なお、応答メッセージｔｍ４７は応答メッセージｔｍ３７、要求メッセージｔｍ４８は要求メッセージｔｍ３８、応答メッセージｔｍ４９は応答メッセージｔｍ３９に対応している。

ＩＰサーバ装置１３において応答メッセージｔｍ４７を生成して以降の動作が、図１８に示す動作と本質的に異なるのは、ＡＤＦ２１６およびＪａｒファイル２１５が処理の対象となる点と、ＡＤＦ２１６に内包されているパッケージＵＲＬ（“http://www.sub.bbb.co.jp/viewer.jar”）で特定されるＪａｒファイル２１５の送信を要求する内容の要求メッセージｔｍ４８が移動機１６にて生成される点と、この要求メッセージｔｍ４８が移動機１６から送信されＩＰサーバ装置１４により受信される点と、ＩＰサーバ装置１４においてＪａｒファイル２１５を内包した応答メッセージｔｍ４９が生成される点と、この応答メッセージｔｍ４９がＩＰサーバ装置１４から送信され移動機１６により受信される点である。

（３）変形例

上述した配信システムでは、ＡＤＦとＪａｒファイルはＩＰサーバ装置から送信するようにしたが、片方または両方を管理サーバ装置から送信してもよい。

また、上述した配信システムでは、移動機は、秘密鍵による署名データと公開鍵とを用いてＳＤＦとＡＤＦの作成者との対応関係の正当性を確認するようにしたが、システムに要求されるセキュリティレベルによっては、ＳＤＦに公開鍵を内包させず、ＩＰサーバ装置においてはＡＤＦに対する秘密鍵を用いた署名を行わず、かつ移動機においては当該確認処理を省略する、という形態とし、移動機およびＩＰサーバ装置における処理量や、移動機と管理サーバ装置およびＩＰサーバ装置との間の通信量を低減するようにしてもよい。

また、上述した配信システムでは、Ｊａｒファイルのハッシュ値を当該Ｊａｒファイルに対応するＡＤＦに内包させる一方、移動機において

ハッシュ値を算出し、両者を比較し、ＪａｒファイルとＡＤＦとの対応関係の正当性を確認するようにしたが、システムに要求されるセキュリティレベルによっては、ＡＤＦにハッシュ値を内包させずに当該確認処理を省略する形態とし、移動機およびＩＰサーバ装置における処理量や移動機とＩＰサーバ装置との間の通信量を低減するようにしてもよい。

また、上述した配信システムでは、トラステッドＪａｖａ－ＡＰに固有のＡＰＩＤを使用してＳＤＦとＡＤＦ（およびＪａｒファイル）との対応が正当であるか否かを判定するようにしたが、トラステッドＪａｖａ－ＡＰを提供する情報提供事業者に固有のＣＩＤを用いてＳＤＦとＡＤＦ（およびＪａｒファイル）との対応が正当であるか否かを判定するようにしてもよい。また、システムに要求されるセキュリティレベルによっては、ＡＰＩＤやＣＩＤを用いた判定を省略するようにしてもよい。

また、上述した配信システムではドメインネームを用いてサーバを指定するようにしたが、ＩＰアドレスを用いてサーバを指定するようにしてもよい。

また、移動機において、ＳＤＦの送信元のサーバ装置のドメインネームを予め設定された文字列と比較し、信頼できる機関が管理するサーバ装置のドメインネームである場合にのみ、ＳＤＦを正当と認める態様としてもよい。この態様では、比較対象の文字列（例えば、通信事業者のドメインネームを示す文字列）は移動機のＲＯＭまたは不揮発性メモリに予め格納されることになる。文字列をＲＯＭに予め格納すれば、文字列の書き換えが不可能であるから、より高いセキュリティを確保できる。また、文字列を不揮発性メモリに予め格納する場合では、移動機の売買後に信頼できる機関を格納することができるので、ユーザおよび信頼できる機関に対して優れた利便性を提供することができる。

また、上述した配信システムでは、ＳＤＦの配信に使用する通信路を提供する通信事業者を信頼できる機関として高いセキュリティを確保するようにしたが、本発明は通信路の提供が信頼できる機関により為さ

れていない態様をも技術的範囲に含む。例えば、信頼できる機関と移動機とを暗号化通信路により接続し、この通信路を介して信頼できる機関がＳＤＦを配信するようにしてもよい。また、通信路のセキュリティが確保されていなくても、ＳＤＦを暗号化した後に配信し、移動機においてＳＤＦを復号するようにすれば、ある程度のセキュリティを確保してＳＤＦを配信することができる。

上述した配信システムでは、ＨＴＴＰに従ってファイルを送受するようにしたが、ＨＴＴＰＳを使用し、より高いセキュリティを確保するようにシステムを変形してもよい。

また、上述した配信システムにおいて、信頼できる機関がＩＰとなってよいこと、すなわち、管理サーバ装置がＩＰサーバ装置を兼ねるようにしてもよい。

さらに、上述した配信システムでは、Ｊａｖａ－ＡＰによる利用を制限する対象としてＡＰＩを挙げたが、任意のリソースを対象とすることができる。ここでいうリソースはハードウェアリソースであってもよい。また、後述するネットワークリソースやソフトウェアリソースであってもよい。ハードウェアリソースとしては、メモリやスピーカ、マイク、赤外線コントローラ、ＬＥＤ（Light Emitting Diode）等の移動機が備え得るものや移動機と共働するＵＩＭ（User Identity Module）やＳＩＭ（Subscriber Identity Module）等の外部機器なども挙げられる。

次にネットワークリソースについて説明する。前述したように、移動機は移動通信網との間で無線通信を行う。この無線通信時には、移動機は、移動通信網により提供される無線チャネル等の無線リソースを使用する。この無線リソースはネットワークリソースの一種である。また、移動機は無線リソースが属する通信プロトコルレイヤよりも高位の通信プロトコルレイヤにおいて、パケットの伝送路や回線接続の通信路などの通信リソースを使用する。このような通信リソースもネットワークリソースの一種である。

次にソフトウェアリソースについて説明する。ソフトウェアリソース

としては、ＡＰＩやクラス、パッケージ等が挙げられる。ソフトウェアリソースが提供する機能は様々であるが、典型的な機能として、暗号演算などの演算処理機能や、Ｗｅｂブラウザ等の他のアプリケーションとの間でデータを送受したりする機能などが挙げられる。また、本発明は、上記外部機器が有するソフトウェアリソースをも利用の制限対象とする態様を技術的範囲に含む。

ところで、Ｊａｖａ－ＡＰによるハードウェアリソースやネットワークリソースの利用は、ソフトウェアリソースを利用して行われるのが一般的である。上述した配信システムにおける移動機も、ハードウェアリソースやネットワークリソースを利用するためのソフトウェアリソースを有しており、このようなソフトウェアリソースの利用を制限することにより、間接的に、ハードウェアリソースやネットワークリソースの利用を制限している。このように、間接的に制限することにより、多様なソフトウェアリソースを用意すれば、トラステッドＪａｖａ－ＡＰについてのみ、Ｊａｖａ－ＡＰの権限を変更する権限を与える、またはダウンロード元のサーバ装置としか通信することができないという制限を外す、あるいは特定の記憶領域に対してアクセスできるようにするといった、複数のリソースの制限を細かく変更しなければ実現できないようなことまで容易に指定できるようになる。なお、移動機に設定されたソフトウェアリソースの利用を制限して上記外部機器のソフトウェアリソースの利用を間接的に制限する態様も本発明の技術的範囲に含まれる。

なお、パーミッションの表現方法としては、一つのリソースと一つのフラグ（許可／禁止）とを対応付けるようにしてもよいし、複数のリソースのパーミッションを一つの表現で示すようにしてもよい。

また、本発明では、複数の種類を持つリソースについて、利用を許可（あるいは禁止）するようにパーミッションを示すことも可能である。この場合、移動機において、より木目細かな制御が実現される。例えば、メモリには２つの形態(読み出しと書き込み)があるから、非トラステッ

ドＪａｖａ－ＡＰには読み出しでしか利用されないが、トラステッドＪａｖａ－ＡＰには読み出し及び書き込みの両方で利用され得るようにすることもできる。また、例えば、１つのパケット伝送路を複数のアプリケーションが共用可能な移動機において、パケット伝送路を利用する権限を有するＪａｖａ－ＡＰが起動されている間にＷｅｂブラウザ等が起動された場合、当該Ｊａｖａ－ＡＰが「パケット伝送路の利用を排他的に行う」ことを許可されていないＪａｖａ－ＡＰであればＷｅｂブラウザ等によるパケット伝送路の共用を排除することはできないが、「パケット伝送路の利用を排他的に行う」ことを許可されているＪａｖａ－ＡＰであればパケット伝送路を占有して使用することができる、といった制御が可能となる。また、上記変形例をさらに変形することで、以下の制御も可能となる。即ち、ある種のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を排他的に利用することが可能となる。また、別のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用するためにはユーザの許可を得ることが必要となる。また、別のパーミッションを与えられたＪａｖａ－ＡＰはユーザに許可を求めることなくパケット通信路を利用することが可能だがパケット通信路を排他的に利用することは不可能となる。また、別のパーミッションを与えられたＪａｖａ－ＡＰはユーザの許可を得て初めてパケット通信路を利用することが可能となる。また、別のパーミッションを与えられたＪａｖａ－ＡＰはパケット通信路を利用することすら不可能となる。これらの例から明らかなように、本発明における「利用の種類」には、リソースを利用する際に経る手順の種類（ユーザの許可を得る手順／ユーザの許可を得ない手順）も含まれる。

また、上述した配信システムでは全ての移動機に対して同一のリストページが提供されるが、移動機毎に異なるリストページを提供するようにしてもよい。

また、上述の配信システムでは、Ｊａｖａ－ＡＰの実行時にＪａｖａ－ＡＰの挙動を制限するようにした。その代わりに、ＩＰサーバ装置に格納されているＪａｒファイルにポリシー情報を内包させ、移動機において、Ｊａｒファイルのダウンロード時に、このポリシー情報とＳＤＦ中とのポリシー情報とを比較し、両者が一致しない場合には、当該Ｊａｒファイルに対応するＪａｖａ－ＡＰを起動できないように、あるいは当該Ｊａｒファイルを含むＪａｖａ－ＡＰソフトウェアをインストールできないようにしてもよい。もちろん、両ポリシー情報の一致する項目についてのパーミッションのみを有効とするようにしてもよい。

また、通信事業者がＣＡにより付与された秘密鍵を用いて署名してからＳＤＦを配信し、移動機においてＣＡが通信事業者に付与した公開鍵を用いてＳＤＦの署名を検証するようにしてもよい。もちろん、通信事業者の公開鍵は予め移動機に格納されていなければならない。公開鍵は、通信により配信し予め不揮発性メモリに書き込むことが可能である。また、ＲＯＭに書き込んだ後に移動機を販売することも可能である。

また、上述の配信システムではソフトウェアは移動機へ配信されるが、本発明の技術的範囲には、移動機以外の端末装置へ配信する態様も含まれる。

請求の範囲

1．　ファイルの格納位置を通知されると当該ファイルを返送する通信システムが、アプリケーションを実現するためのソフトウェアを内包した実体ファイルに依存した情報と前記実体ファイルの格納位置を示す情報とを含んだアプリケーション記述ファイルの格納位置を示す第１の識別情報と、前記ソフトウェアに従って実行されるアプリケーションの挙動の許容範囲に関する権限情報とを内包したセキュリティ記述ファイルを、当該ファイルを格納した管理サーバ装置から前記セキュリティを確保して前記権限情報によって示された範囲内でアプリケーションの挙動を許可する端末装置へ送信する権限送信過程と、

前記端末装置が、前記権限送信過程にて前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第１の識別情報を用いて、前記アプリケーション記述ファイルを記憶した１または複数のサーバ装置から、当該アプリケーション記述ファイルを取得する依存情報取得過程と、

前記端末装置が、前記依存情報取得過程にて取得した前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得するプログラム取得過程と

を有する配信方法。

2．　前記アプリケーション記述ファイルが、前記依存情報取得過程にて前記管理サーバ装置から取得される請求項１に記載の配信方法。

3．　前記実体ファイルが、前記プログラム取得過程にて前記管理サーバ装置から取得される請求項１に記載の配信方法。

4．　前記アプリケーション記述ファイルが前記依存情報取得過程にて

前記管理サーバ装置から取得され、

前記実体ファイルが前記プログラム取得過程にて前記管理サーバ装置から取得される請求項１に記載の配信方法。

５．　前記通信システムが前記セキュリティ記述ファイルを暗号化する暗号化過程と、

前記端末装置が、前記権限送信過程にて前記通信システムから送信された前記セキュリティ記述ファイルを復号する復号過程とを有し、

前記権限送信過程では、前記暗号化過程にて暗号化された前記セキュリティ記述ファイルを前記端末装置へ送信し、

前記依存情報取得過程では、前記端末装置が、前記復号過程にて復号された前記セキュリティ記述ファイルを用いて前記アプリケーション記述ファイルを取得する

請求項１に記載の配信方法。

６．　前記権限情報は資源の利用に関する制限を示す

請求項１に記載の配信方法。

７．　前記資源は前記端末装置内部のハードウェア資源である

請求項６に記載の配信方法。

８．　前記資源は前記端末装置外部の、前記端末装置が使用可能なハードウェア資源である

請求項６に記載の配信方法。

９．　前記資源は前記端末装置内部のソフトウェア資源である

請求項６に記載の配信方法。

１０．　前記資源は前記端末装置外部の、前記端末装置が使用可能なソ

フトウェア資源である
請求項６に記載の配信方法。

１１．前記資源は、前記端末装置が使用可能なネットワーク資源である
請求項６に記載の配信方法。

１２．前記権限情報は資源の利用の種類を示す
請求項１に記載の配信方法。

１３．前記アプリケーションに対応するアプリケーション記述ファイルは前記アプリケーションを提供する情報提供事業者に対して認証局が与えた秘密鍵で署名されており、
前記アプリケーションに対応するセキュリティ記述ファイルは前記情報提供事業者に対して認証局が与えた公開鍵を内包し、
前記プログラム取得過程では、前記端末装置が、前記依存情報取得過程で取得したアプリケーション記述ファイルの正当性を前記公開鍵を用いて検証し、正当性が検証された場合にのみ、当該アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する
請求項１に記載の配信方法。

１４．前記アプリケーション記述ファイルおよび前記セキュリティ記述ファイルは、前記管理サーバ装置を管理する管理者が付与するアプリケーション識別子を内包し、
前記プログラム取得過程では、前記端末装置が、前記権限送信過程で前記管理サーバ装置から送信されたセキュリティ記述ファイルに内包されたアプリケーション識別子と前記依存情報取得過程で取得したアプリケーション記述ファイルに内包されたアプリケーション識別子と

を比較し、両者が一致した場合にのみ、当該アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

請求項１に記載の配信方法。

１５．　前記通信システムは、さらに、前記セキュリティ記述ファイルの格納位置を示す第２の識別情報を内包したダウンロード用ファイルを格納した情報提供サーバ装置を有し、

前記通信システムが端末装置へ前記ダウンロード用ファイルを送信する事前送信過程と、

前記端末装置が、前記事前送信過程にて前記通信システムから送信された前記ダウンロード用ファイルを用いて前記セキュリティ記述ファイルの送信を前記通信システムに要求する権限送信要求過程とを有し、

前記権限送信過程では、前記通信システムが、前記権限送信要求過程にて要求された前記セキュリティ記述ファイルを前記端末装置へ送信する

請求項１に記載の配信方法。

１６．　前記依存情報送信過程にて送信されるセキュリティ記述ファイルの格納位置が前記管理サーバ装置内の場合にのみ前記依存情報取得過程以降の過程を実行する

請求項１に記載の配信方法。

１７．前記端末装置は移動機である

請求項１～請求項１６のいずれか一の請求項に記載の配信方法。

１８．　アプリケーションを実現するためのソフトウェアを内包した実体ファイルと、前記実体ファイルに依存した内容を有し前記実体ファイルの格納位置を示すアプリケーション記述ファイルとを格納した１または複数のサーバ装置と、前記アプリケーション記述ファイルの格納位

置を示す第１の識別情報と端末装置が前記ソフトウェアを実行することにより実現されるアプリケーションに与えられた権限を示す権限情報とを内包したセキュリティー記述ファイルを格納した管理サーバ装置とを有し、ファイルの格納位置を通知されると当該ファイルを返送する通信システムと、

アプリケーションに与えられた権限に応じた挙動を当該アプリケーションに対して許可する端末装置とを有し、

前記管理サーバ装置は、前記セキュリティ記述ファイルを前記端末装置へ、セキュリティを確保して送信し、

前記端末装置は、前記通信システムから送信された前記セキュリティ記述ファイルに内包されている前記第１の識別情報を用いて前記アプリケーション記述ファイルを取得し、前記アプリケーション記述ファイルを用いて前記通信システムから前記実体ファイルを取得する

配信システム。

１９．　前記管理サーバ装置が前記アプリケーション記述ファイルを格納する請求項１８に記載の配信システム。

２０．　前記管理サーバ装置が前記実体ファイルを格納する請求項１８に記載の配信システム。

２１．　前記管理サーバ装置が前記アプリケーション記述ファイルを格納し、

前記管理サーバ装置が前記実体ファイルを格納する請求項１８に記載の配信システム。

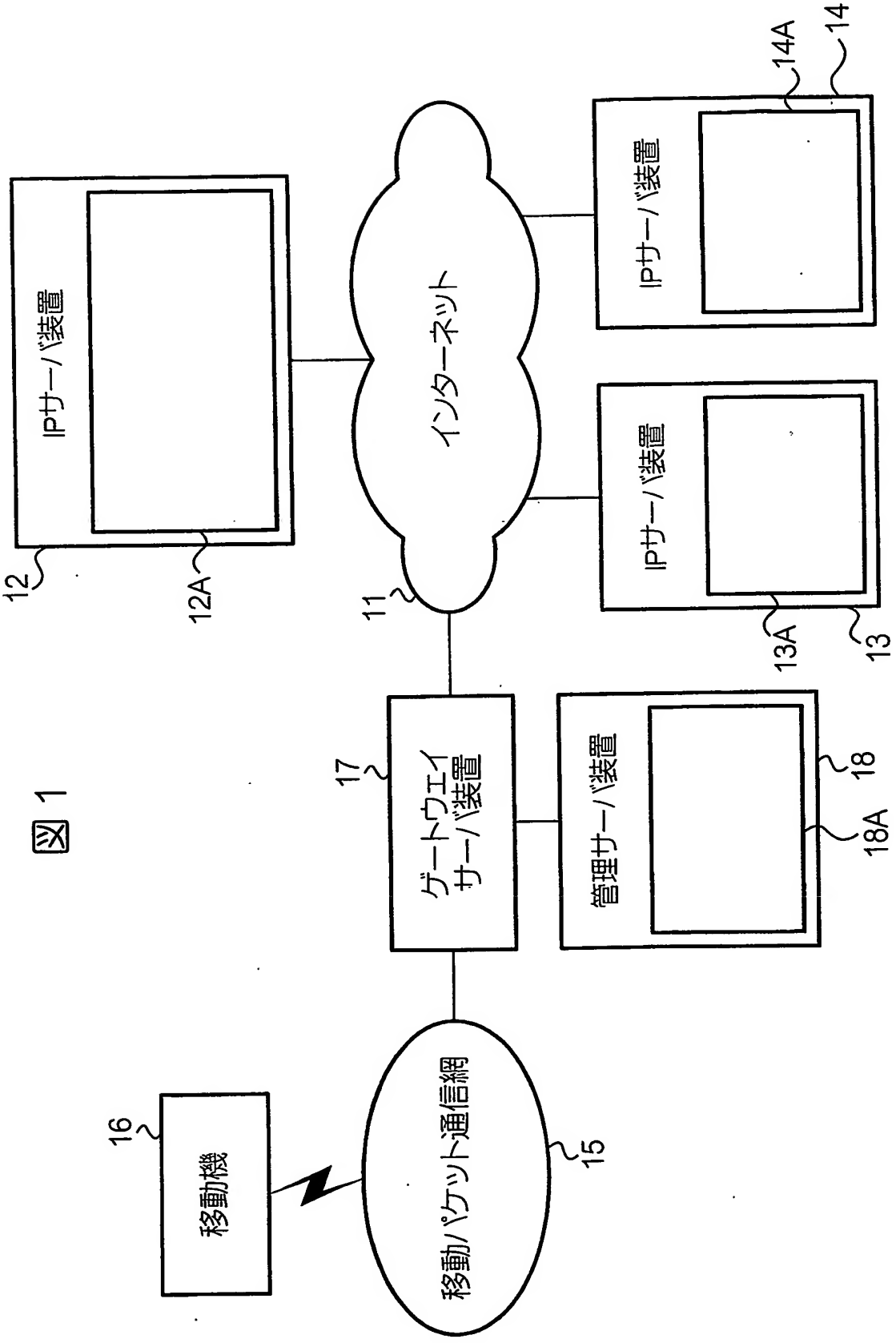

IPサーバ装置
12
12A
インターネット
11
IPサーバ装置
14A
14
IPサーバ装置
13A
13
ゲートウエイ
サーバ装置
17
管理サーバ装置
18
18A
移動機
16
移動パケット通信網
15

図1

図 2

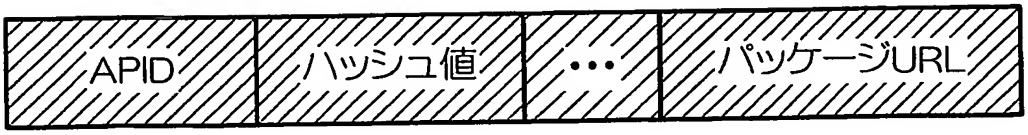

APID
ハッシュ値
・・・
パッケージURL

図 3

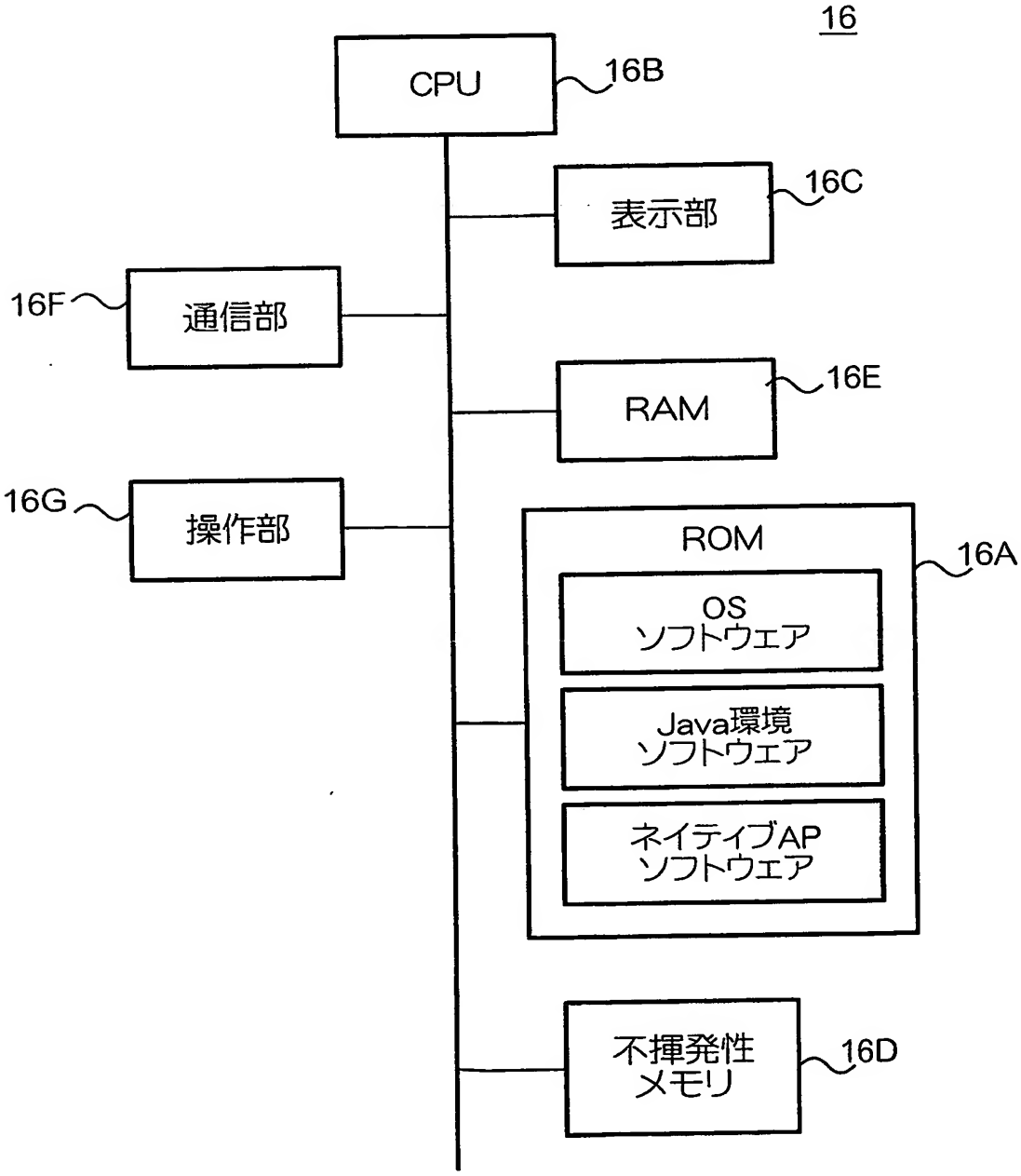

16
CPU
16B
表示部
16C
16F
通信部
RAM
16E
16G
操作部
ROM
16A
OS
ソフトウェア
Java環境
ソフトウェア
ネイティブAP
ソフトウェア
不揮発性
メモリ
16D

図4

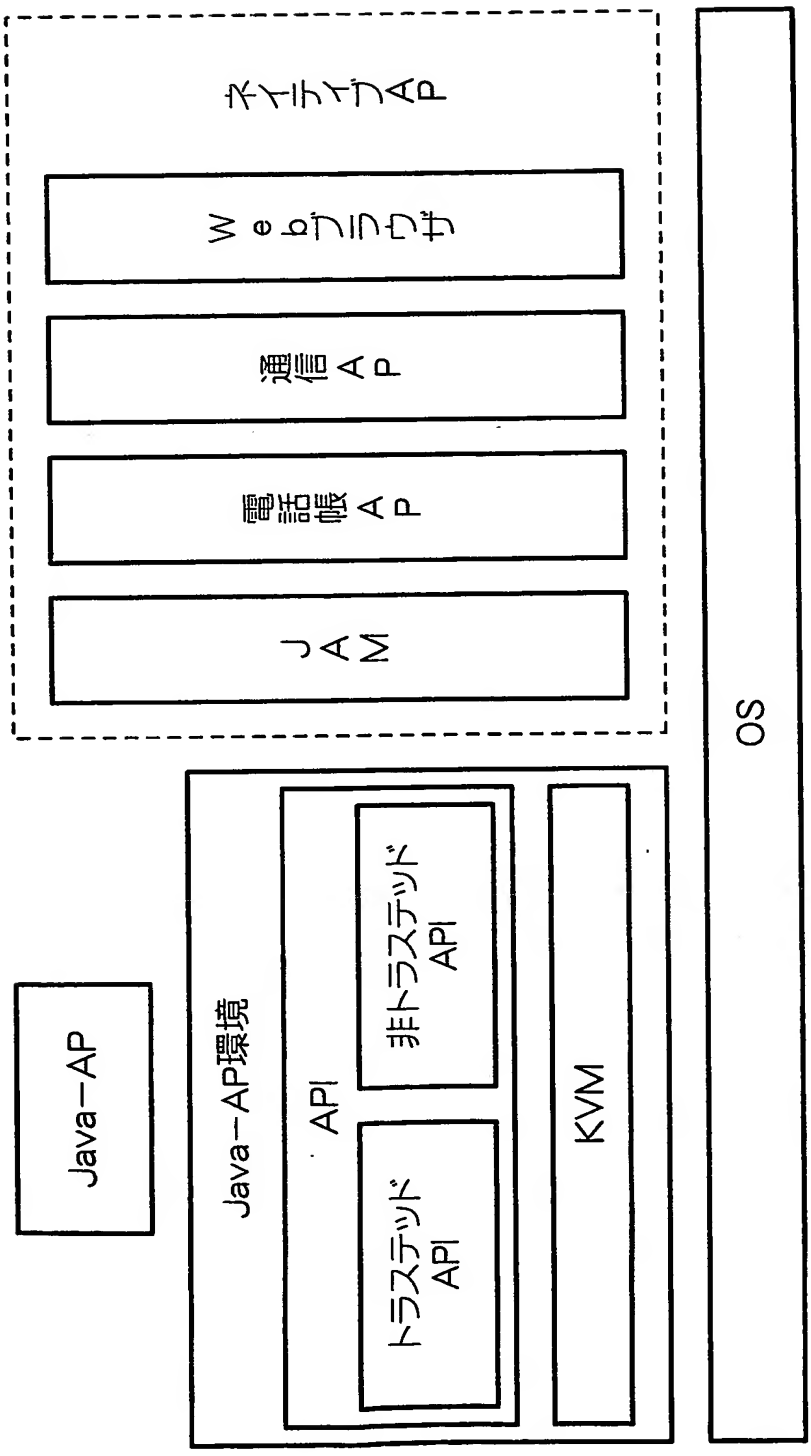

ネイティブAP
Webブラウザ
通信AP
電話帳AP
JAM
OS
Java−AP
Java−AP環境
API
トラステッドAPI
非トラステッドAPI
KVM

図 5

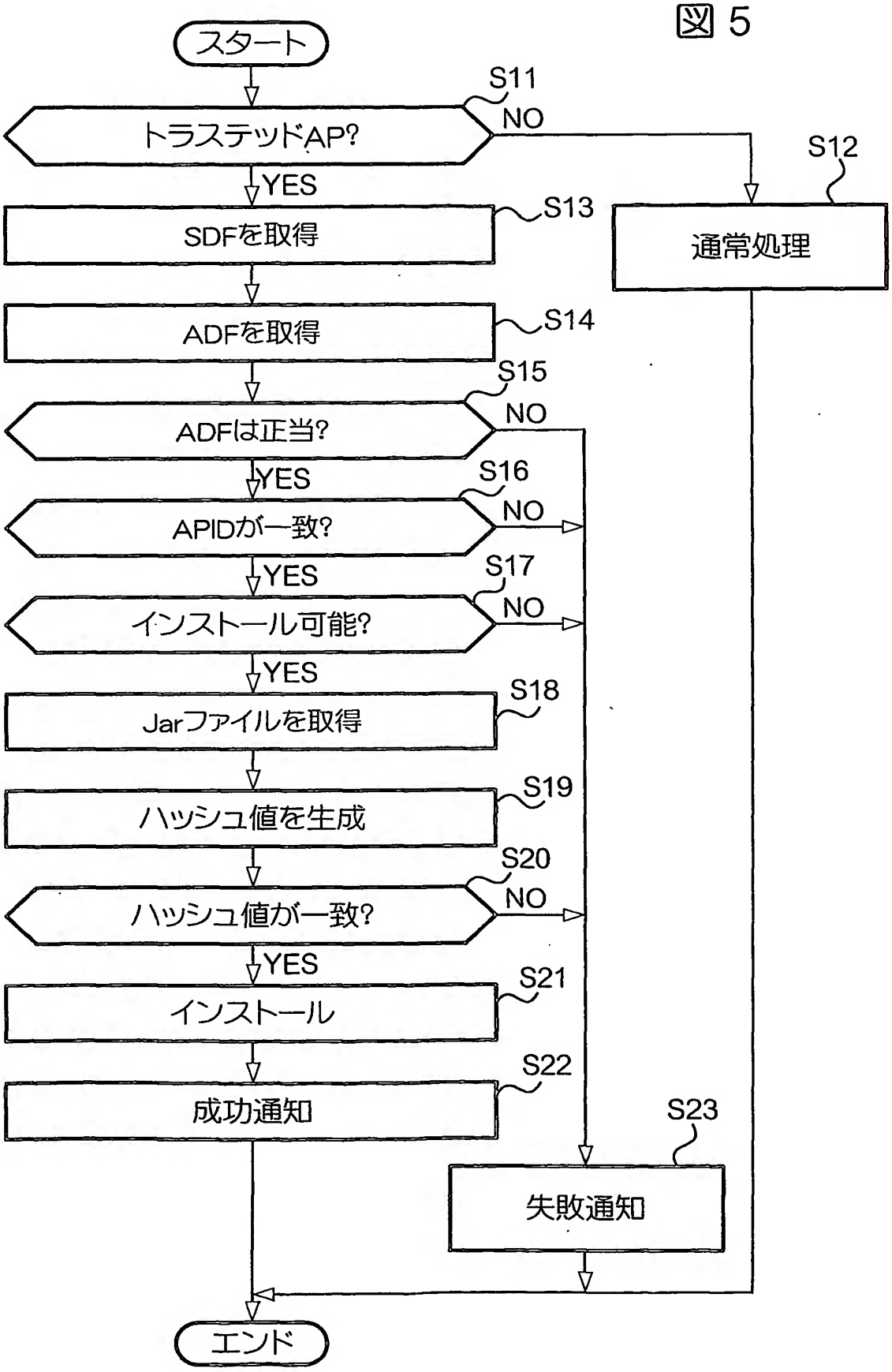

スタート
S11
トラステッドAP?
NO
S12
YES
S13
SDFを取得
通常処理
S14
ADFを取得
S15
ADFは正当?
NO
YES
S16
APIDが一致?
NO
YES
S17
インストール可能?
NO
YES
S18
Jarファイルを取得
S19
ハッシュ値を生成
S20
ハッシュ値が一致?
NO
YES
S21
インストール
S22
成功通知
S23
失敗通知
エンド

図 6

APID	ポリシー情報	ADF－URL	公開鍵

図 7

トラステッドAPI	パーミッション
getPhoneList()	○
getCallHistory()	×
getMsStatus()	○

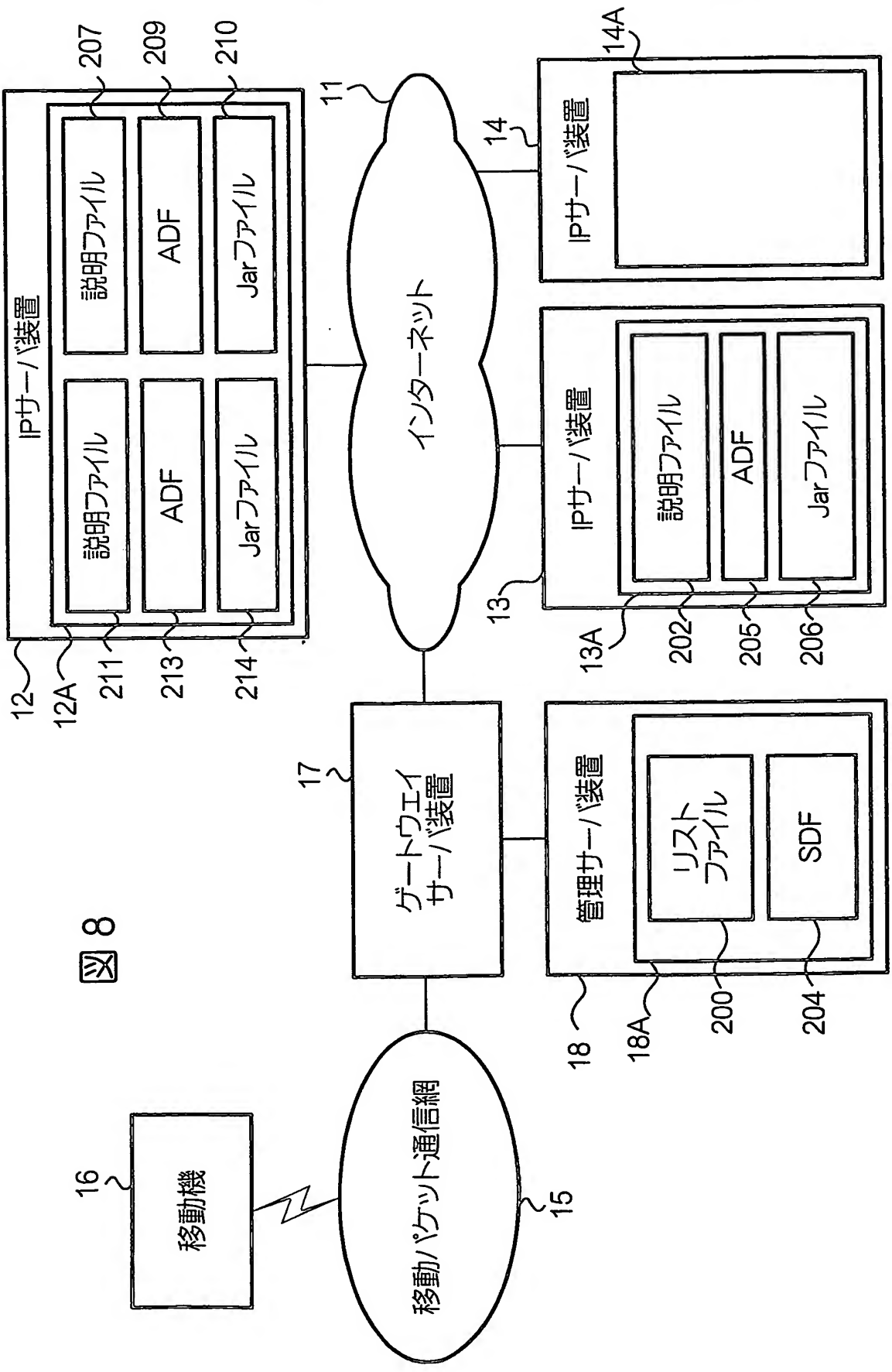

16
移動機
15
移動パケット通信網
17
ゲートウェイ
サーバ装置
11
インターネット
18
18A
管理サーバ装置
リスト
ファイル
SDF
200
204
14
14A
IPサーバ装置
13
13A
IPサーバ装置
説明ファイル
ADF
Jarファイル
202
205
206
12
12A
IPサーバ装置
説明ファイル
ADF
Jarファイル
211
213
214
207
209
210

図 8

図 9

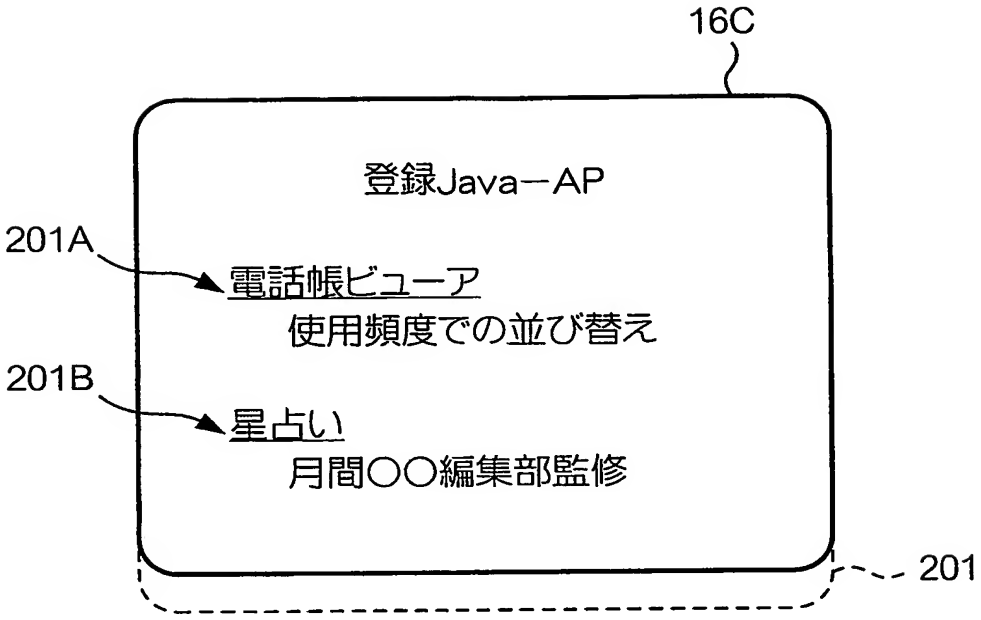


図 10

<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/horoscope.jam>
詰め将棋
</OBJECT>
～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。

図 11

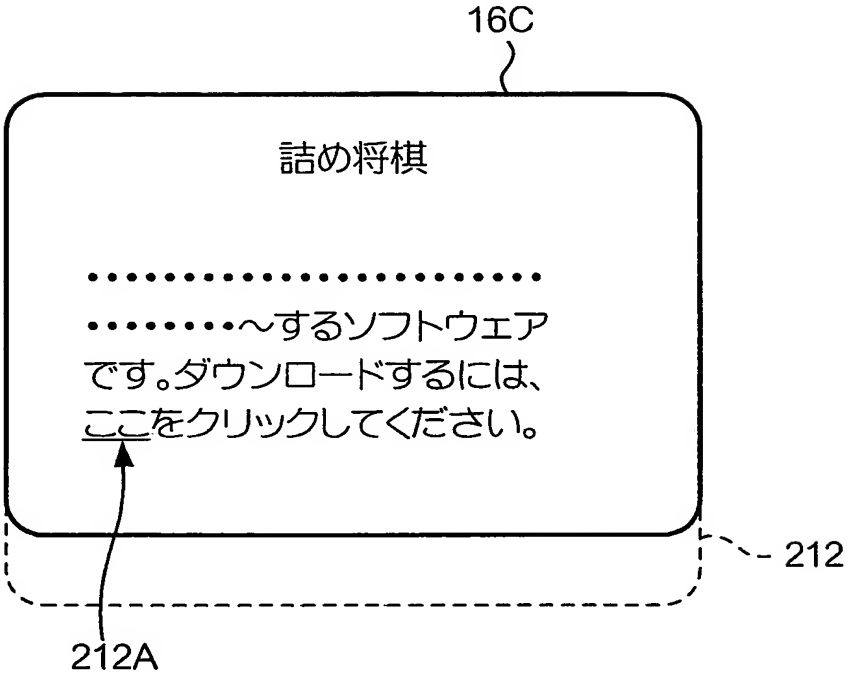


図 12

<OBJECT declare id="application.declaration"
data="http://www.ccc.co.jp/viewer.jam>
星占い
</OBJECT>
～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。

図 13

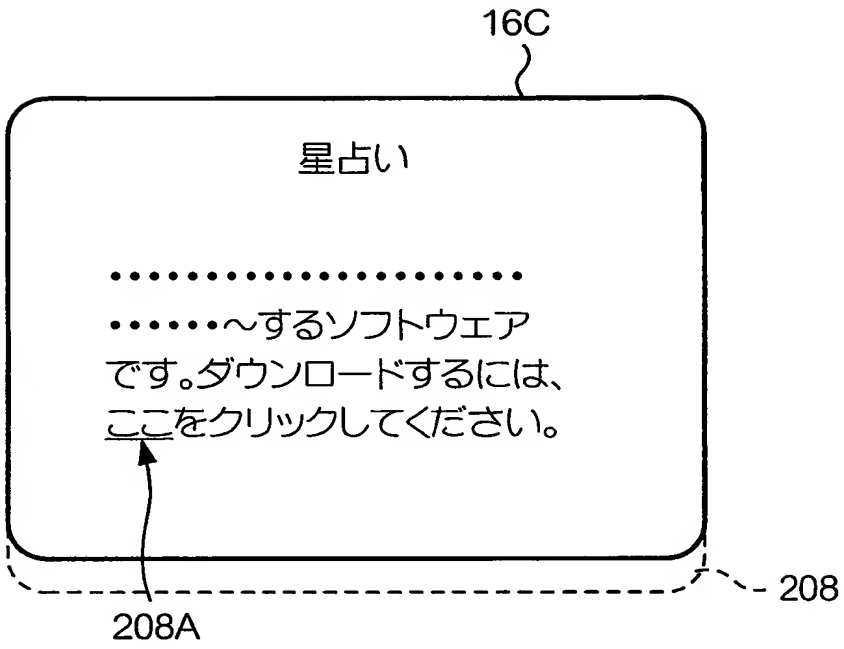


図 14

```
<OBJECT declare id="application.declaration"
data="http://www.aaa.co.jp/abc.sdf"
type="application/x-jam">
電話帳ビューア
</OBJECT>
  ～するソフトウェアです。ダウンロードするには
<A ijam="#application.declaration">ここ</A>
をクリック。
```

図 15

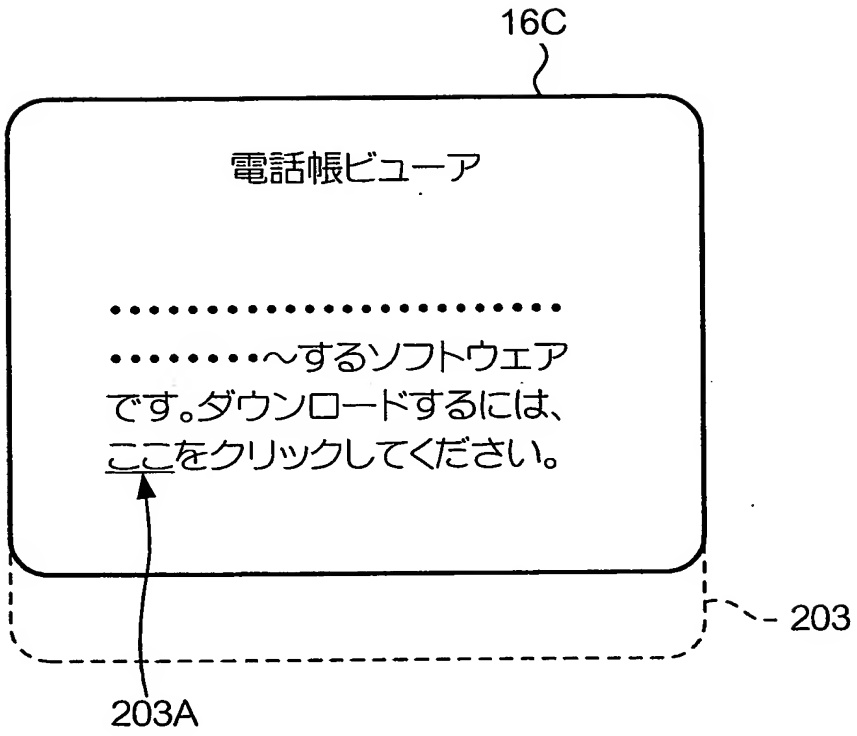

16C
電話帳ビューア
・・・・・・・・・・・・・・・・・・・・・・・・
・・・・・・・・～するソフトウェア
です。ダウンロードするには、
ここをクリックしてください。
203
203A

図 16

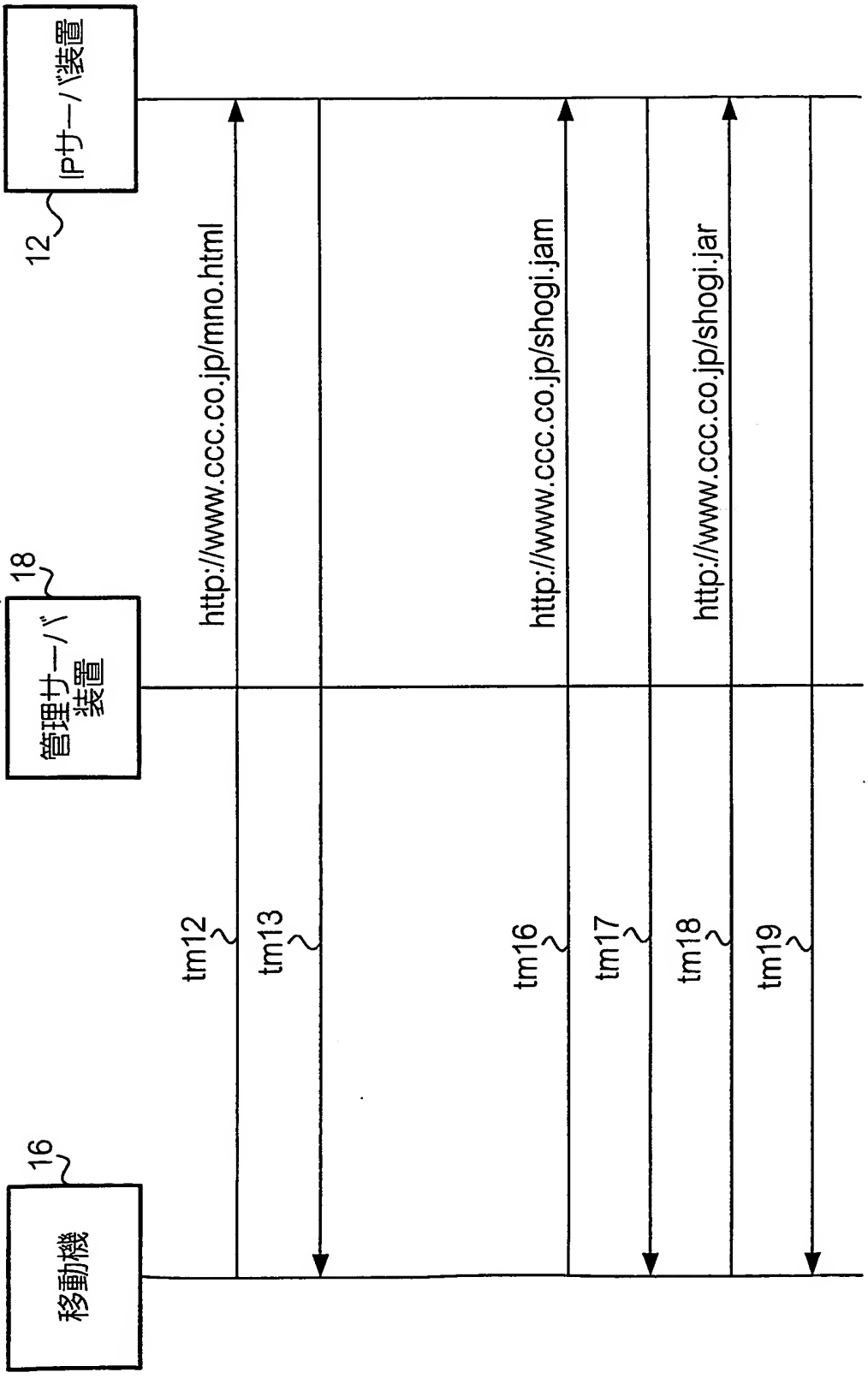

移動機
16
管理サーバ装置
18
IPサーバ装置
12
http://www.ccc.co.jp/mno.html
http://www.ccc.co.jp/shogi.jam
http://www.ccc.co.jp/shogi.jar
tm12
tm13
tm16
tm17
tm18
tm19

図 17

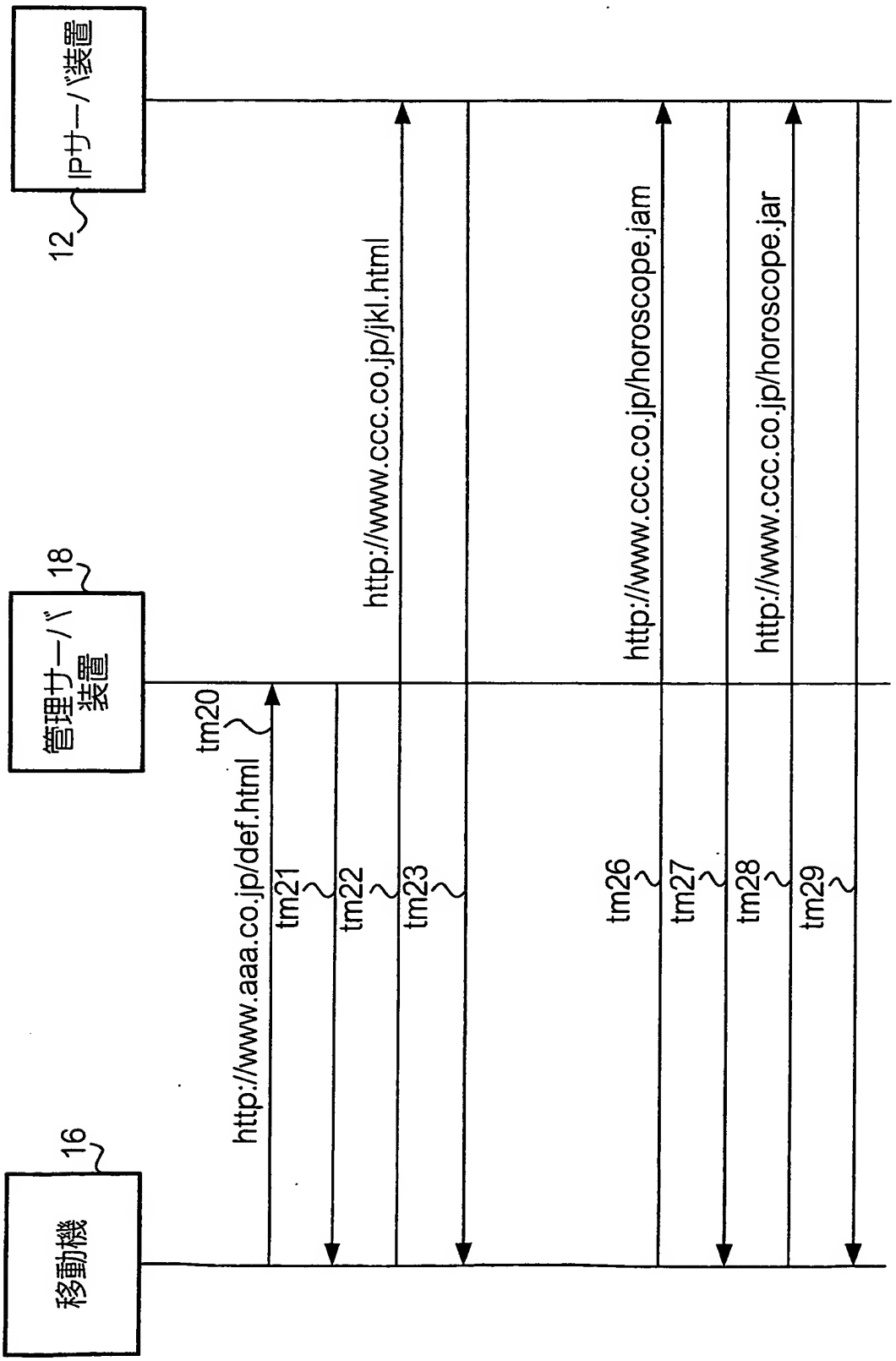

移動機
16
管理サーバ装置
18
IPサーバ装置
12
tm20
http://www.aaa.co.jp/def.html
tm21
tm22
tm23
http://www.ccc.co.jp/jkl.html
tm26
tm27
http://www.ccc.co.jp/horoscope.jam
tm28
tm29
http://www.ccc.co.jp/horoscope.jar

図 18

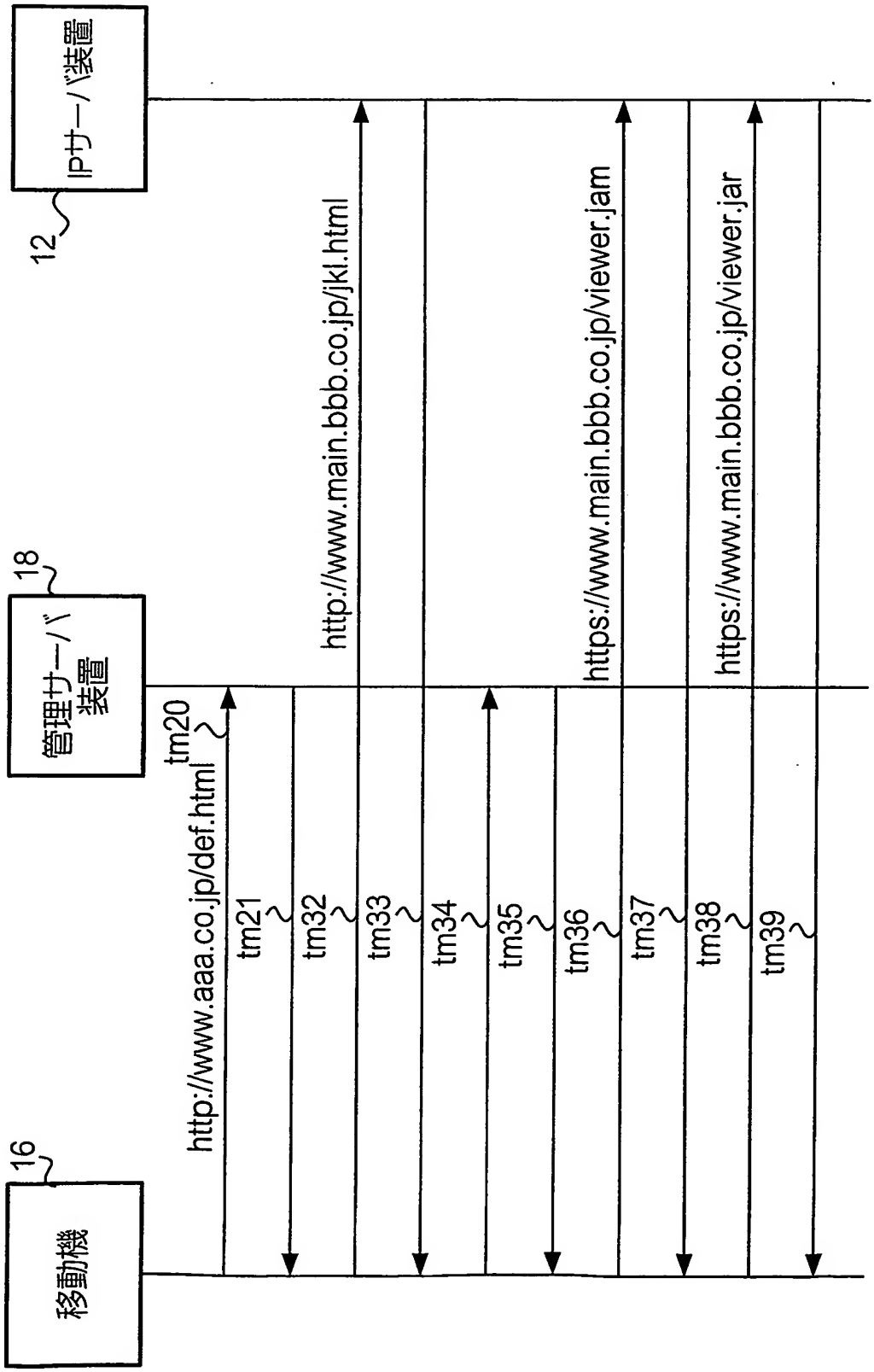

移動機
16
管理サーバ装置
18
IPサーバ装置
12
http://www.aaa.co.jp/def.html
tm20
http://www.main.bbb.co.jp/jkl.html
https://www.main.bbb.co.jp/viewer.jam
https://www.main.bbb.co.jp/viewer.jar
tm21
tm32
tm33
tm34
tm35
tm36
tm37
tm38
tm39

図 19

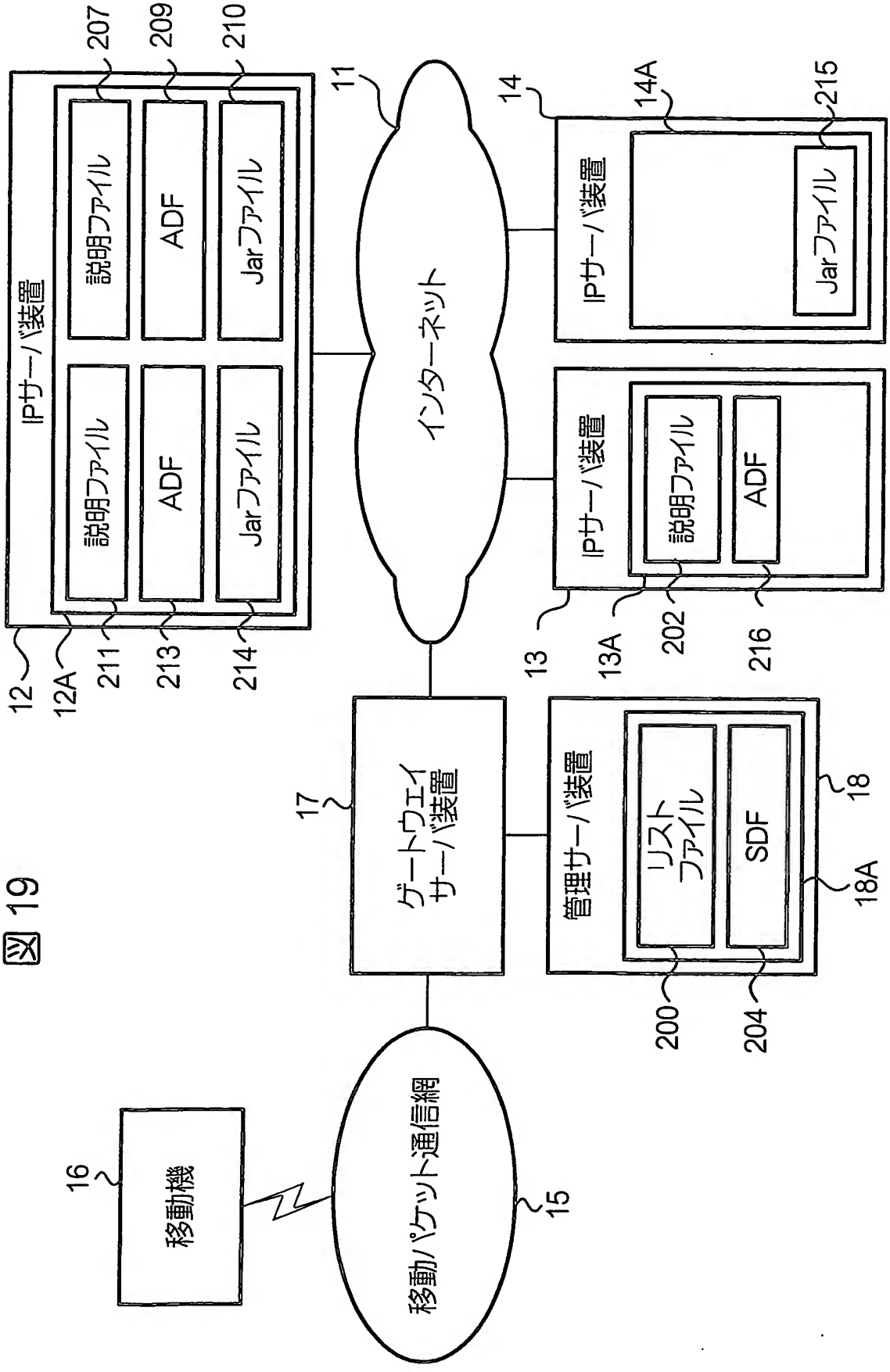
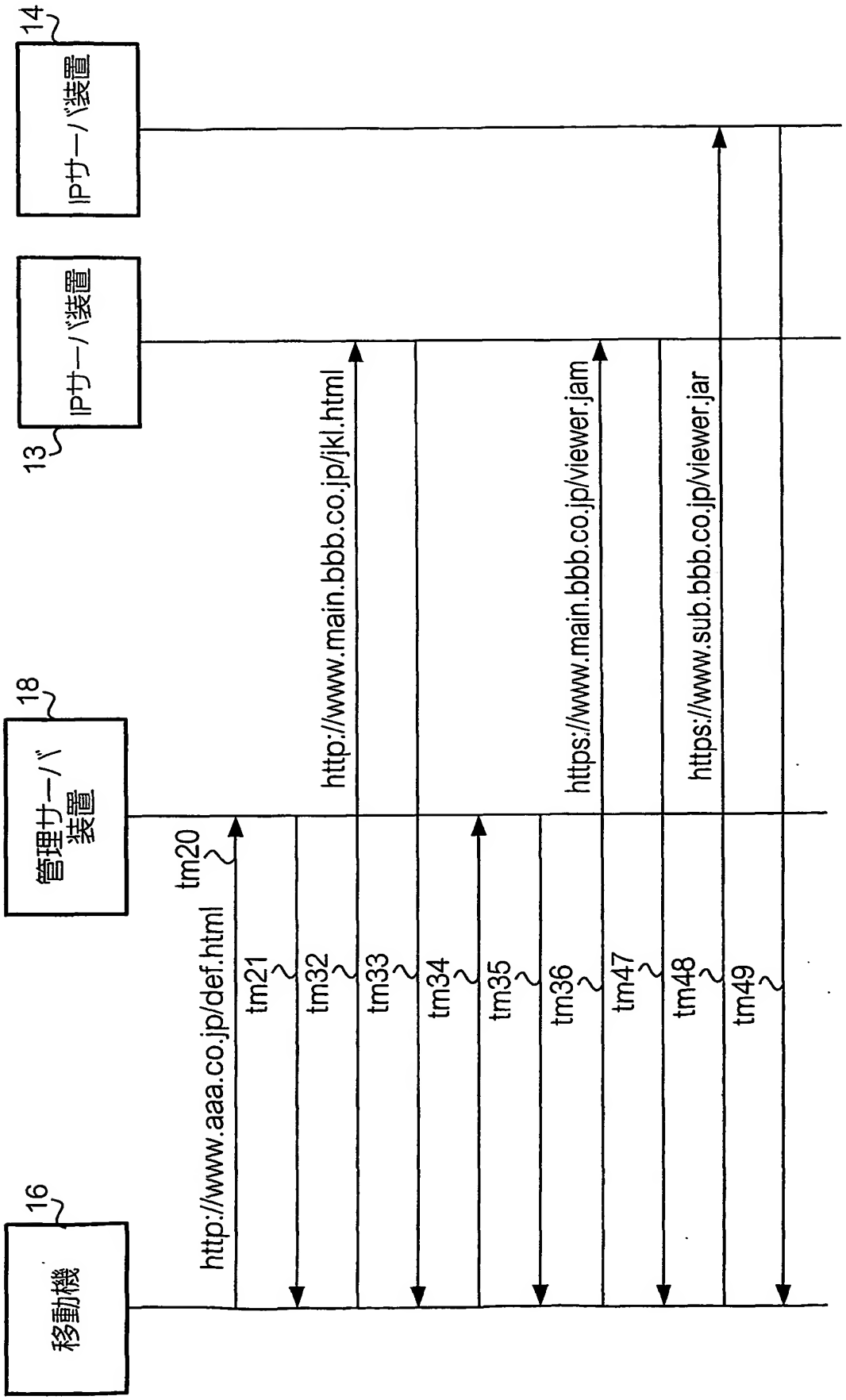

IPサーバ装置
説明ファイル
ADF
Jarファイル
インターネット
IPサーバ装置
Jarファイル
IPサーバ装置
説明ファイル
ADF
ゲートウェイ
サーバ装置
管理サーバ装置
リスト
ファイル
SDF
移動パケット通信網
移動機
12
12A
211
213
214
207
209
210
11
14
14A
215
13
13A
202
216
17
18
18A
200
204
15
16

図 20


移動機
16
管理サーバ装置
18
IPサーバ装置
13
IPサーバ装置
14
http://www.aaa.co.jp/def.html
tm20
tm21
tm32
http://www.main.bbb.co.jp/jkl.html
tm33
tm34
https://www.main.bbb.co.jp/viewer.jam
tm35
tm36
tm47
https://www.sub.bbb.co.jp/viewer.jar
tm48
tm49

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/00035

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F1/00, 9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F1/00, 9/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98/021683 A2 (FINJAN SOFTWARE, LTD.), 22 May, 1998 (22.05.98), Full text; all drawings & WO 99/035583 A2 & US 6092194 A & US 6154844 A & US 6167520 A & EP 965094 A & IL 129729 D & JP 2003-514326 A Full text; all drawings	1-21
A	WO 00/042498 A1 (Hitachi, Ltd.), 20 July, 2000 (20.07.00), Full text; all drawings & AU 1889699 A	1-21

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 03 April, 2003 (03.04.03)	Date of mailing of the international search report 15 April, 2003 (15.04.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/[redacted]03/00035

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6317742 B1 (Sun Microsystems, Inc.), 13 November, 2001 (13.11.01), Full text; all drawings & EP 853279 A2 & SG 085092 A & JP 10-254783 A Full text; all drawings	1-21
A	JP 2001-243062 A (Nippon Telegraph And Telephone Corp.), 07 September, 2001 (07.09.01), Full text; all drawings (Family: none)	1-21
A	JP 2001-117769 A (Matsushita Electric Industrial Co., Ltd.), 27 April, 2001 (27.04.01), Full text; all drawings (Family: none)	1-21
A	Tetsuya KAKU, Masahiro YAMADA, Hiroaki ITO, "Hajimete no i-mode Java Programming Junbi kara Haifu made 'i Appli' Kaihatsu no Subete", first edition, Introduction to Java Programming in i-mode, 26 March, 2001 (26.03.01), pages 37 to 41	1-21
A	"21 Seiki ni Mukete DoCoMo no Mobile Multimedia no Sekai i-mode o Sarani Omoshiroku, 'i Appli' Service & 503i Series", Business Communication, 01 February, 2001 (01.02.01), Vol.38, No.2, pages 44 to 47	1-21
A	Jemie Jaworski, "Java 2 Security Programming Kiso Gainen kara Jisso no Shosai made Shoban", Java Security Handbook, 1st Edition, 25 April, 2001 (25.04.01), pages 79 to 90, 529 to 541	1-21
E,A	JP 2003-50641 A (NEC Corp.), 21 February, 2003 (21.02.03), Full text; all drawings (Family: none)	1-21

国際調査報告 [redacted]　　国際出願番号　PCT/[redacted]03/00035

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl⁷　G06F1/00, 9/06

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl⁷　G06F1/00, 9/06

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　１９２２－１９９６年
日本国公開実用新案公報　１９７１－２００３年
日本国登録実用新案公報　１９９４－２００３年
日本国実用新案登録公報　１９９６－２００３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	WO 98/021683 A2(FINJAN SOFTWARE,LTD.) 1998.05.22,全文,全図 & WO 99/035583 A2 & US 6092194 A & US 6154844 A & US 6167520 A & EP 965094 A & IL 129729 D & JP 2003-514326 A 全文,全図	1-21
A	WO 00/042498 A1(株式会社日立製作所 HITACHI,LTD.) 2000.07.20,全文,全図 & AU 1889699 A	1-21

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
03.04.03	15.04.03

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）		
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	中野　裕二　印	5B	9462
	電話番号　０３－３５８１－１１０１　内線　３５４５		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

国際調査報告 [redacted]　　国際出願番号　PCT/[redacted]03/00035

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	US 6317742 B1(Sun Microsystems, Inc.) 2001.11.13, 全文, 全図 & EP 853279 A2 & SG 085092 A & JP 10-254783 A 全文, 全図	1-21
A	JP 2001-243062 A(日本電信電話株式会社) 2001.09.07, 全文, 全図(ファミリーなし)	1-21
A	JP 2001-117769 A(松下電器産業株式会社) 2001.04.27, 全文, 全図(ファミリーなし)	1-21
A	加来 徹也, 山田 昌宏, 伊藤 広明, はじめてのｉモードＪａｖａプログラミング 準備から配布まで「ｉアプリ」開発のすべて 1版 Introduction to Java programming in i-mode, 2001.03.26, p37-41	1-21
A	21世紀に向けて ＤｏＣｏＭｏのモバイルマルチメディアの世界 ｉモードをさらに面白く、「ｉアプリ」サービス＆５０３ｉシリーズ，ビジネスコミュニケーション，2001.02.01，第38巻，第2号，p44-47	1-21
A	ジョウォルスキー ジェミー Jemie Jaworski, Ｊａｖａ２セキュリティプログラミング 基礎概念から実装の詳細まで 初版 Java Security Handbook, 1st Edition, 2001.04.25, p79-90, 529-541	1-21
EA	JP 2003-50641 A(日本電気株式会社) 2003.02.21, 全文, 全図(ファミリーなし)	1-21